世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G06F 15/00, G06K 19/00, E05B 49/00	A1	(11) 国際公開番号	WO99/60485
		(43) 国際公開日	1999年11月25日(25.11.99)

(21) 国際出願番号 PCT/JP99/02599

(22) 国際出願日 1999年5月19日(19.05.99)

(30) 優先権データ

特願平10/139563	1998年5月21日(21.05.98)	JP
特願平10/299181	1998年10月21日(21.10.98)	JP
特願平10/323129	1998年11月13日(13.11.98)	JP
特願平10/361752	1998年12月21日(21.12.98)	JP

(71) 出願人；および
(72) 発明者
保倉 豊(YASUKURA, Yutaka)[JP/JP]
〒276-0025 千葉県八千代市勝田台南二丁目15番22号
Chiba, (JP)
(74) 代理人
関 正治(SEKI, Masaharu)
〒102-0076 東京都千代田区五番町4番地 幸ビル4階
Tokyo, (JP)

(81) 指定国 AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

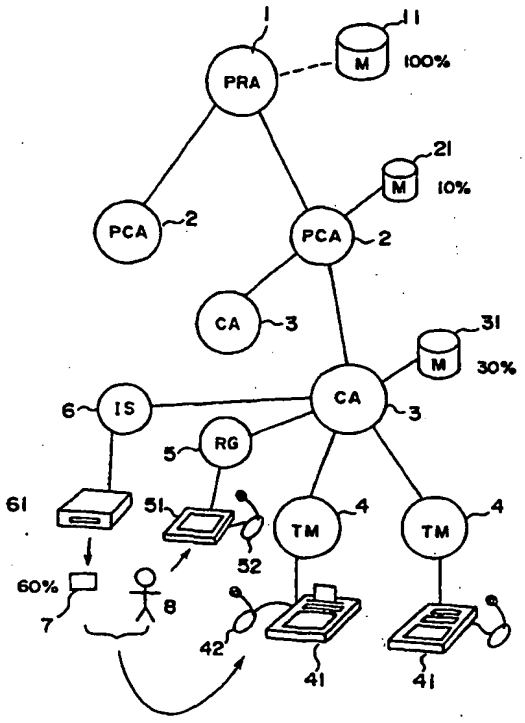
添付公開書類
国際調査報告書

(54)Title: AUTHENTICATION CARD SYSTEM

(54)発明の名称 認証カードシステム

(57) Abstract

Biological feature data, such as handwriting or sound spectrogram, for identifying the user (8) is acquired, and then a user authentication voucher (7) on which at least part of the biological feature data is recorded is issued. By comparing the contents recorded on the user authentication voucher (7) read by an authentication voucher reader (41) with the user's biological feature data inputted into an authentication acquisition device, an authentication use office (4) authenticates the user directly. Authentication stations (2, 3) are installed to record part of the biological feature of the user in each authentication station. In response to an inquiry of the authentication use office (4), additional authentication is made to improve the reliability of authentication. An authentication IC card used in this system includes a CPU, an authentication file where authentication information is stored, and application files sorted according to the depth of authentication.



(57)要約

ユーザ（８）の個体を区別する筆跡声紋等の生物学的特徴データを取得して該生物学的特徴データの少なくとも一部を記録したユーザ認証票（７）を発行し、認証票読取り装置（４１）で読み取ったユーザ認証票（７）の記録内容と人証取得装置に入力されたユーザの生物学的特徴データを比較することにより認証利用所（４）で直接にユーザ認証する。また認証局（２）、（３）を備え、ユーザの生物学的情報の一部を各認証局毎に記録しておいて、認証利用所（４）の照会に応えて追加認証することにより認証の信頼性を向上させる。なお、本システムに使用する認証ＩＣカードは、ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備える。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦
AL アルバニア
AM アルメニア
AT オーストリア
AU オーストラリア
AZ アゼルバイジャン
BA ボズニア・ヘルツェゴビナ
BB バルバドス
BE ベルギー
BF ブルギナ・ファソ
BG ブルガリア
BJ ベナン
BR ブラジル
BY ベラルーシ
CA カナダ
CF 中央アフリカ
CG コンゴー
CH スイス
CI コートジボアール
CM カメルーン
CN 中国
CR コスタ・リカ
CU キューバ
CY キプロス
CZ チェッコ
DE ドイツ
DK デンマーク
DM ドミニカ
EE エストニア
ES スペイン
FI フィンランド
FR フランス
GA ガボン
GB 英国
GD グレナダ
GE グルジア
GH ガーナ
GN ガンビア
GR ギニア
GW ギニア・ビサオ
HR ギリシャ
HU クロアチア
ID ハンガリー
IE インドネシア
IL アイルランド
IN イスラエル
IS インド
IT アイスランド
JP イタリア
KE 日本
KG ケニア
KP キルギスタン
KR 北朝鮮
KZ 韓国
LC カザフスタン
LI セントルシア
LK リヒテンシュタイン
LR スリ・ランカ
LS リベリア
LT レソト
LU リトアニア
LV ルクセンブルグ
MA ラトヴィア
MC モロッコ
MD モナコ
MG モルドヴァ
MK マダガスカル
ML マケドニア旧ユーゴスラヴィア共和国
MN マリ
MR モンゴル
MW モーリタニア
MX マラウイ
NE メキシコ
NL ニジェール
NO オランダ
NZ ノールウェー
PL ニュー・ジーランド
PT ポーランド
RO ポルトガル
RU ルーマニア
SD ロシア
SE スーダン
SG スウェーデン
SI シンガポール
SK スロヴェニア
SN スロヴァキア
ST シエラ・レオネ
SZ セネガル
TD スワジランド
TG チャード
TJ トーゴー
TM タジキスタン
TR タンザニア
TT トルクメニスタン
UA トルコ
UG トリニダッド・トバゴ
US ウクライナ
UZ ウガンダ
VN 米国
YU ウズベキスタン
ZA ヴィェトナム
ZW ユーゴースラビア
南アフリカ共和国
ジンバブエ

明細書

認証カードシステム

技術分野

この発明は、電子情報交換や電子商取引における個人認証を行うためのユーザ認証システムと、これに用いるユーザ認証票、およびユーザ認証装置、さらにこれを適用して予め認可された特定の者にのみ開閉を許すようにした錠前管理システムに関する。

背景技術

近年、通信網を介してアクセスする情報の種類は極めて多様になりつつあり、商品の売買やクレジット決済などの電子商取引は勿論、医療におけるオンライン診断や個人カルテ、役所における登録事項の閲覧、証明書の発行など、対象もますます増加し、利用が進む傾向にある。

こうした個人的な情報にはプライバシーに係わり他人に漏洩する危険性がある場合には開示してはならないとされるものが少なくない。電子情報通信網の発達を取り込んでより便利な情報社会を構築するために、個々人を峻別できる信頼性の高いユーザ認証方式が求められている。

また、個人を正しく認証する機構は、研究所や事業所あるいは住宅などにおける資格者以外の立ち入りを制限する施錠装置などや、電子マネーのセキュリティ向上にも利用することができる。

従来、ユーザ認証にはパスワードが最もよく用いられてきた。パスワードは簡便であるが、他人のパスワードを盗用して本人に成りすます者を排除することができない。このため、長いパスワードを使う、推測しにくいパスワードを選ぶ、パスワードを時々変更するなど、相応の注意をして安全性を確保しようとする。また、通信過程における安全性を確保するためには暗号化技術を用いて通信内容を秘密化して、データの漏洩があっても他人に容易に内容を知られないようにすることも広く行われている。

しかしそれでも、通信の盗聴や暗号文の解読や盗み見などによりパスワードを

盗まれることがあり、完全に安全なものとは成り得ない。また、安全性を考慮してパスワードを複雑にするほど利用者自身がそれを正確に記憶しておくことが困難になる欠点がある。さらに本質的には、どれほど複雑なパスワードであっても、それがデジタルデータとして蓄えられた瞬間から何らかの手段により複製することが可能になるという性質がある。

なりすましを防止し本人であることを確実に認証するため、指紋や声紋など、いわゆる生物学的特徴を表す情報を用いてユーザ認証する方法も検討されている。しかし、一般に生物学的特徴データは情報量が大きいため認証を必要とする利用現場とユーザの生物的情報を蓄積している認証局の間で膨大な通信量を交換しなければならない。したがって、通信路の輻輳や通信時間の長大化のため特殊な環境における場合以外には実用化することが困難であり、かつそのデータの管理場所と管理方法に問題があった。

近年、研究所や事業所、研究室、資料保管室さらに住宅など、セキュリティの確保のため特定の場所に出入りできる者を限定し、有資格者に発行したカードによる認証に合格した場合だけ開錠する施錠管理システムがよく用いられている。

また、商品の販売やクレジット決済などの電子商取引、医療におけるオンライン診察、個人カルテや役所における登録事項の閲覧、証明書の発行など、本人にのみ取引を認めるべき場合に本人認証を正確に行う必要がある。さらにこのような場合に対面して取引を行うのでなく、通信網を利用して情報にアクセスする機会が多くなりかつ多様化している。

こうした取引では真正な取引対象者であるか否かを判定しなければならず、また、場合によっては対面交渉なしに本人であるか否かを正確に判断できなくてはならない。これらの場合、カードを仲介にして本人認証を行うことで信頼性を向上させることができる。

なお、取引の種類により要求されるセキュリティの程度が異なるため、必要とされる本人認証の深さが異なる。たとえば少額商品を販売する場合にはカードの純正が保証できれば満足できても、医療用カルテの発行に利用する場合は確実に本人であることが証明できる顔写真、指紋、声紋などの生物学的情報を併用することが好ましい。

施錠管理や入退場管理に用いられる鍵カードは、通常錠前毎に発行され、有資格者が所持あるいは管理する。したがって多数の部屋などを入退場管理の対象とする場合は、高度の資格者は多数の鍵カードを所持しなくてはならず管理が煩雑になる。なお、１枚の鍵カードを有資格者が共有して利用することも多いが、この場合は暗証番号や鍵カードの管理を厳重に行わなければ認可されていない者の盗用を許すことになり、かえって安全の保持が困難になる。

また、取引用カードも取引毎に取引関係者間で合意の下に発行されるもので、個人が所有する取引用カードの数はいつの間にか膨大な数になってしまうきらいがある。

貸ロッカーなどでもカードを鍵として利用するシステムがあるが、ロッカー毎に鍵を準備しこれを貸与する方式であるため、本来の利用者と異なる者が鍵を使ってもロッカーの開閉ができるので、保管物が他人に盗取られる可能性があり、安全性は十分でない。

より高度な保護を行う貸金庫などでは、金庫を貸すときに提供した鍵と管理者の鍵と合わせて始めて解錠できるようにしたものがあるが、管理者が同席する必要があるうえ、盗まれたり複製された鍵を用いても解錠でき安全性も十分ではない。

また、錠前に入力するダイヤルやキーボードを設けて、ロックするときに暗号を決めて同じ暗号を入力しなければ解錠できないようにした金庫もある。こうした金庫類では鍵を持ち歩く必要がなく、使用者が利用の度に設定する暗号に基づいて解錠するので、簡単でありながら安全性が高いが、暗号を盗み見たり推理や試行により解読して解錠される可能性が残る。

さらに、研究室、資料保管室、薬品保管庫など、セキュリティの確保のため出入りできる者を限定し、有資格者に発行したカードによる認証に合格したときだけ解錠する錠前管理システムもあるが、このシステムではカードの管理が杜撰であると無資格者がカードを使用して自由に出入りするようになる畏れがある。

なお、アクセスする錠前により要求されるセキュリティの程度が異なるため、何でも高い安全性を追求して利用者に煩雑な手続を要求することは避けなくてはならない。たとえば猛毒物を管理する棚を開けるためには多少煩雑でも確実な認

証を必要とするが、持ち出し量を管理することで十分な通常の薬品を取り出すためには簡単な確認で十分である。

貸金庫でも掛替えのない貴重品や高価な財物を収納したときと、いくらでも手に入る品物を収納したときでは、安全保証の要求水準が異なる。

一方、近年ＩＣカードなどＣＰＵと記憶装置を内蔵するカードをクレジットカードや電子マネーなどに利用するようになってきた。

ＩＣカードは高度な認証に伴う複雑な演算も可能であり記録内容の書き換えが容易であることが特徴で、取引の経緯を逐次記録できるカードや電子マネーとして使用することなどに適している。

また、ＩＣカードなどに内蔵される記憶容量が大きくなってきたため、カード自体に各種の個人的情報を記録して携帯することも可能となっている。常時携帯することが便利な個人的情報には保険証番号、クレジットの利用者番号、社員証番号や社内における経歴、電子マネー残額、戸籍簿の内容、病歴、さらに住所録など、プライバシーに係わり他人に対する秘匿性を確保しなくてはならないものがある。

このような認証ＩＣカードは、カードに記録された情報に基づいて本人認証をおこなうため、カードのセキュリティが大きな問題となる。

そこで、本発明は、電子情報交換や電子商取引における個人認証を行うための安全性が高く迅速に結果が得られるユーザ認証システムと、これに用いられるユーザ認証票およびユーザ認証装置を提供することを目的とする。

また、本発明は、取引や施錠システムのセキュリティ向上のために対象毎に発行してきた認証カードを資格者認証として統合した認証ＩＣカードを提供することを目的とし、さらに、ＩＣカード自体に格納する情報に対するアクセスの安全が保証されプライバシー保護が万全な認証ＩＣカードを提供することを目的とする。

また、本発明は、有資格者を厳格に判定して安全性が高い錠前管理システムを提供し、必要に応じて有資格者認証の深さを設定できる錠前管理システムを提供することを目的とする。

発明の開示

本発明のユーザ認証システムは、登録所と認証票発行所と認証利用所と少なくとも１個の認証局を備える。登録所はユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えており、認証票発行所はユーザに対してその生物学的特徴データの少なくとも一部を記録したユーザ認証票を発行し、認証利用所はユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを取得する人証取得装置を設けている。また、認証局は認証利用所と情報通信路で接続されたおり、登録所において取得したユーザの生物学的特徴データのうちユーザ認証票に記録しない部分を記録しておく。そして、認証利用所の認証票読取り装置で読みとったユーザ認証票の記録内容と人証取得装置で取得したユーザの生物学的特徴データを比較することによりユーザ認証すると共に、さらに高度な認証が必要なときに認証局で認証利用所からの照会に応えてユーザ認証票において欠けている生物学的特徴データの部分を比較して認証した結果を認証利用所に送付して認証を行うことを特徴とする。

なお、本明細書では、人の意志により制御しきれないため他人と区別できるような個体に固有の特徴を生物学的特徴という。このような生物学的特徴には、指紋や掌紋、虹彩や網膜のパターン、ＤＮＡ情報など生来のもののみならず、筆跡、声紋など習慣などにより形成されるものもあり、今後もより確実で容易に認識できる生物学的特徴が見出される可能性がある。

また、本発明第２のユーザ認証システムは、登録所と認証票発行所と認証利用所を備え、ユーザ認証票に演算機能を備え、認証利用所で生物学的特徴データを取得してユーザ認証票に入力すると、ユーザ認証票の演算機能を用いて、ユーザ認証票に記録されている生物学的特徴データと人証取得装置で取得されたユーザの生物学的特徴データを比較し、またさらに認証局の認証結果を統合することによりユーザ認証票の正当な所有者であることを認証することを特徴とする。

本発明のユーザ認証システムは、さらに、認証利用所と情報通信路で接続された少なくとも１個の認証局を備え、ユーザ認証票には登録所において取得したユーザの生物学的特徴データの一部を除いて記録しておき、ユーザ認証票に記録しない部分を各認証局に記録しておいて、認証利用所からの照会に応えてユーザ認

証票において不足する生物学的特徴データの部分を比較して認証するようにすることが好ましい。

さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えてもよい。

本発明のユーザ認証システムは、ユーザの個体を区別する生物学的特徴データの少なくとも一部を記録したユーザ認証票を使用し、認証が必要なときには、ユーザが入力した生物学的特徴データとユーザ認証票の生物学的特徴データを比較することによりユーザ認証するため、ユーザ自身でなければ認証テストをパスすることができないのでなりすましを防止できる。

また、デジタルデータ化された生物学的特徴データから元の生物学的特徴データを復元することは極めて難しいばかりか、たとえ復元ができてもその生物学的特徴を他人が複製することはできないため、ユーザ認証の信頼性が極めて高い。

特に、ユーザ認証票に照会用の生物学的特徴データを記録しているため、遠隔の認証局でユーザ認証をしてもらわなくても、認証を必要とする認証利用所において本人であることを直接確認することができる。このため認証局との通信に多大な時間および費用を費やす必要がない。

なお、ユーザ認証票内にＣＰＵやＲＡＭなど演算機能を備えて、ユーザ認証票を利用しようとするユーザから取得した生物学的特徴データを入力し記録されている情報と対照するようにしたときは、認証利用所の負担を軽減し装置コストを低減しより利用しやすいシステムとすることができ、また、ユーザ認証票内で情報処理を完結させて認証票の外部に認証データが漏洩するのを防ぎ安全性を向上させることができる。

さらに、ユーザ認証票と認証局で生物学的特徴データを分割して記録しておく場合は、必要情報が分割されているので、例えば認証票に記録されたデータから生物学的特徴データを復元しても認証システムを突破することはできないし、ユーザ認証票から認証に用いるデータを複製することもできないので、安全である。また、たとえユーザ認証票の記憶内容を改竄しても認証局における情報が保全されているため他人のなりすましを排除することができる。

なお、本発明の方法は分割されたデータを１箇所に集めて再統合して判定する

従来の分割方式と異なり、認証利用所と認証局がそれぞれ手元の生物学的特徴データに基づいて認証を行った結果を利用するものであって、元のデータ全体が再現されることがないので、データの秘密が保持され安全性が極めて高い。

あるいはまた、認証局がアタックされた場合にもユーザの所有するユーザ認証票の情報まで改竄することができないため安全である。

また、複数の認証局を用いて、ユーザ認証票の情報に基づいたユーザ認証に加えて、各認証局毎に認証利用所もしくは他の認証局からの照会に応えて認証するようにした場合は、例えば階層的に組織された認証局のユーザ認証を段階的に取得することによりユーザ認証の信頼性をより高くすることができる。

なお、本発明のユーザ認証システムでは、要求される認証信頼性の水準に従い、ユーザ認証票に記録された情報に基づき認証利用所のみの認証で合否決定することを選択することも、ユーザ認証票に記録されていない情報を加味した認証局における認証を追加してより確実な判定を選択することも可能である。

このような認証のレベルは認証利用所や取引対象により予め決めておいてもよく、取引毎に認証利用所で設定してもよい。さらに、取引価額などに伴い自動的に選択して設定できるようにしてもよい。

また、この情報分割方式によれば、たとえ生物学的特徴データの全部を用いてユーザ認証を行う場合でも、大部分についてユーザ認証票中の情報を用いて認証利用所で認証を行うようにすれば、通信回路を介して交換する情報量は小部分になり通信回路容量も小さくてよくまた照会に掛かる時間も少ない。なお、情報を分割することは、多数のユーザについて情報を集積しておき多数の照会を処理しなければならない認証局における処理能力や記憶容量の要求を抑制する効果もある。

さらに、ユーザ認証システムには登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認定登録局を備えて、登録所において取得したユーザの生物学的特徴データの全容を記録しておくことにより、何らかの不正使用や異常が起きた場所の判定、あるいは認証票が破損したときの再発行、下位の認証局のデータの補修などに利用することができる。なお、ユーザが認証票を携帯しない場合にも、認証局における記録に基づいてある程度信頼の置ける認

証を得ることができる。たとえば盗難にあったときには、認証局のデータに基づいて本人認証を受けたユーザは、盗まれた認証票の使用を差し止めたり再発行を請求することができる。

また、認定登録局における生物学的特徴データを記録した記憶媒体がユーザ認証システムの情報通信路から切り離せるようにしておいて必要なときだけ接続して使用するようにすれば、ハッカーの侵入などにより個人情報が漏洩したり改竄されたりすることを防止することができる。なお、ユーザ認証票や下位の認証局にはそれぞれ部分的な生物学的特徴データのみを記録し完全な記録を残さないようにすることが安全性を確保するために極めて有効である。

本発明のユーザ認証システムで使用する生物学的特徴データとして入力過程を加味した筆跡を用いてもよい。筆跡は個人の生物学的特徴をよく表して他人のなりすましが難しく、かつ入力する装置および解析する装置が比較的容易に得られるという利点がある。ユーザを識別するために書いて貰う文字や図形は適当なものでよいが、自己の氏名を表すサインなどは再現性がよいため好ましいのはいうまでもない。書き上がった筆跡は他人が真似することができるが、書き順や筆勢など入力過程を加味することにより個体の生物的特徴が現れるため他人には真似できなくなる。そこで、オンライン入力装置を用いて入力中の情報を加味して判定することにより信頼性の高い認証が可能になる。

また、利用可能な生物学的特徴データには、この他、指紋や掌紋、声紋、虹彩や網膜のパターン、ＤＮＡ情報などがある。また、将来、より確実で容易に認識できる生物学的特徴が見出される可能性がある。

なお、ユーザ認証票と認証局で生物学的特徴データを分割して記録する場合に、情報データを物理的に分割して前半部分をユーザ認証票に記録し、後半部分を認証局に記録して照合するようにしてもよく、また、例えば筆跡の形状情報をユーザ認証票に記録し筆圧情報や筆順情報を認証局に記録するなど、情報を階層的にとらえて分割する方法を用いてもよい。

さらに、サインと声紋など複数の生物学的特徴データを別々に記録し、それぞれ異なる種類の情報に基づいて判断することにより信頼性を向上させることも可能である。

なお、生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うように構成しても良い。

正規の生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにすれば、例えば、他人に脅かされて意志に反してサインをせざるを得ない事態に陥った場合にサインのどこかに隠し記号を付け加えると、強要者には素直にサインをしているように見せかけて実は警備金杜に通報をするといった仕組みにすることもできる。

なお、システム構築上の選択として、このような場合に人身上の安全を確保するため、扉の開閉や現金の引出など普通に取引が成立しているように見せかけるようにすることも可能である。こうした目的に使用する生物学的特徴データは正式なものと同じ種類のものであっても良いし、例えばサインに対して音声データを付加するなど異なる種類のものを複合しても良い。また、逆に、疑似データに特定の符合データを付加したものを正式な認証用データとしても良い。

本発明のユーザ認証システムに使用するユーザ認証票は、認識票を識別する信号とユーザの個体を区別する生物学的特徴データの少なくとも一部を記録した読出し可能な記憶領域を備えた記憶媒体からなることを特徴とする。

記憶媒体として、ＲＯＭやＣＤ－ＲＯＭなど読み取り専用の記録媒体を使用してもよいが、記録内容が使用者の生物学的特徴を表す情報であるため改竄の危険が少ないので、取引内容や新たな情報を追加して記録できる書き込み読み取り共に可能な記憶媒体を採用することも可能である。

特に高い偽造防止機能と大きなデータ容量を有し、インテリジェント機能と暗号システムを搭載したセキュリティ機能が高いＩＣカードを利用することが好ましい。

また、ＣＰＵやＲＡＭを搭載したＩＣカードを用いる場合は、ユーザから取得した生物学的特徴データをカード内に取り込んで、内部に記憶した照会用データと比較してユーザ認証を行うようにすれば、認証利用所の負担を軽減し装置コストを低減することができる。また、外部からユーザ認証票の認証データを読み出せないようにして安全性を向上させることができる。

なお、ＩＣカードを使用することにより複合的な機能を搭載し高度な本人認証

機能を有する多目的カードにすることができる。ここで使用するＩＣカードは、外部端子により読み書きする接触式と外部端子によらず非接触で読み書きする非接触式を複合した複合ＩＣカードであってもよい。

特に情報を分散して用いる場合は、ユーザ認証票の記録内容を改竄しても役に立たないので、ユーザ認識票に経済的で簡便なフロッピーディスクを使用してもよい。また、この他にも、ＣＤ－ＲＯＭ、ＤＶＤ、録音テープ、ＭＤ等、書き込み可能な各種の記録媒体が使用できる。

また、本人認証を行うためにＩＣカードを用いた認証ＩＣカードは、ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ＩＣカードであって、外部からアプリケーションファイルに記録された情報の提示要求があったときに、外部から入力される人証情報と認証ファイルに格納された人証情報と対比して認証の深さを確認し、合格したときに初めてＣＰＵを介してアプリケーションファイルの情報を提示することを特徴とする。

従来、認証が必要となる場面毎に独立したカードを発行して対処してきたのは、その方がシステムとして単純で扱いやすいこと、多様な取引者同士の提携が困難なことなどの理由の他に、取引により必要とされる認証の深さが異なり一様な人証情報では対処できないこと、１枚のカードで複数の取引を可能とするとカード所有者に認めたくない資格権限を与えることになる場合が生ずることなどの技術的な障害もあったからである。

本発明の認証ＩＣカードによれば、カード内のアプリケーションファイルをファイル毎に機密性に対応した認証の深さに応じて分類しておき、外部からファイルに記録された情報の提示要求があったときには、入力される人証情報をＣＰＵが対照確認し、ファイルについて予め決められた深さに対応する認証が得られたときにのみＣＰＵを介して目的のアプリケーションファイルの情報を提示するようになっている。

なお、カードの携帯者により入力された人証情報とカード内部に記録された人証情報の照合は、カードから提供した人証情報や予め記憶された人証情報を用いて外部装置によって行うこともできる。外部装置の能力を利用することにより、

複雑な画像処理や情報処理を必要とするときにも対処できるので、認証ＩＣカードのＣＰＵ能力やメモリ容量では不足がある場合などに有効である。また、分割記憶された人証情報を利用することにより信頼性の高い認証を行うことができる。

なお、認証ファイルに格納される人証情報はＩＣカードの真正な所有者の個体を区別する生物学的情報を含むようにすることができる。

また、認証の深さで分類されたアプリケーションファイルには各種取引に用いられるＩＤを記録しであってもよい。このようなＩＤは、外部に取引情報が存在する場合などにおいて、カードの携帯者がこれにアクセスする資格を有するか否かを検証する必要がある場合に有効である。

さらに、アプリケーションファイルに所有者の個人的情報を記録しておいてもよい。本発明の認証ＩＣカードの認証能力は高く本人の承認なしではカード内の個人的情報にアクセスできないので、プライバシーの保護は万全である。

また、アプリケーションファイル毎に予めアクセス資格を登録し、認定された資格者しかファイルへのアクセスを認めない機構を併用しても良い。認証レベルと組み合わせてファイルを２次元的に配設することができるので、より複雑な要求に応えることが可能となる。

本発明の認証ＩＣカードを使用するときは、まず認証ＩＣカード中のアプリケーションファイルに入室許可証、銀行のＩＤなどを格納すると共に、それぞれが要求する認証方法を指定しておく。一方、認証に必要な人証情報を認証ファイルに格納しておく。

たとえば、建物の入場には特別な認証は必要なく適正な認証ＩＣカードを所持していればよいとし、執務室への入室には認証ＩＣカードと共に保持者の真正を確認するため暗証番号が合致しなければならないとし、さらに、資料室への入室にはより厳密な認証が要求され各人の指紋を照合するものとする。

このような場合、認証ファイルに、純正なカードであることを示す情報と暗証番号と保持者の指紋情報を記録しておき、アプリケーションファイルの各々に、建物の入口扉を開扉するために要求される暗号信号と執務室の開扉に必要な暗号信号と資料室の扉を開扉する暗号信号を格納しておく。

カードの携帯者が建物の扉に付属するカード読み取り器に認証ＩＣカードを読

BNSDOCID: <WO_____9960485A1_I >

み取らせると、カード読み取り器がカード情報を取得してカードが真正であって暗号が一致することを確認し、検査に合格したときに扉が開き入場できる。

執務室の扉に設けられたカード読み取り器にはキーボードが付属していて、入室しようとする者は認証ＩＣカードを読み取らせて暗証番号を入力する必要がある。認証カードが真正で暗証番号が認証ＩＣカードの認証ファイルに記録された暗証番号と合致したときに、ＣＰＵを介して開扉に必要な暗号信号がカード読み取り器に送り込まれ、これが正しければ入室が許可される。

また、資料室の扉には指紋読み取り装置を付属したカード読み取り器が設けられていて、入室しようとする者は真正な認証ＩＣカードをカード読み取り器に読み取らせて指定された指を指紋読み取り装置に押し付ける必要がある。指紋が認証ファイルに記録された指紋情報と対応する場合に、ＣＰＵを介して開扉を指示する暗号がカード読み取り器に供給され、この暗号信号がカード読み取り器により真正な者と判定されたときに始めて扉が開いて入室ができる。

同じ仕組みは、金融システムにおいても使用することができる。

クレジット決済を使用する場合にも、低額商品の購入にいちいちサイン入力を要求するのでは煩雑に過ぎて利用価値が減少する。一方、宝飾類など高額な取引では厳重な本人認証を行う必要がある。クレジット決済の利用者認証番号をアプリケーションファイルから出力するにも要求される認証水準が異なるが、本発明の認証ＩＣカードでこれら異なる水準の認証に対応することができる。

また、アプリケーションファイル毎に予めアクセス資格を登録し、認定された資格者しかファイルへのアクセスを認めないようにして、カード読み取り器からの情報アクセスを必要な部分に制限して余分なプライバシー開示を行わないようにすることができる。

たとえば解錠システムが要求できる情報は人証情報と解錠のための暗号信号だけで、医療カルテが格納されているファイルに対するアクセスはＣＰＵによって排除される。場合によっては、不当なアクセス要求があったときには情報交換全てを遮断して情報窃取や改竄を防止するようにすることができる。

本発明の認証ＩＣカードは、サービスや取引毎に利用資格を与えられた者が所持する認証ＩＣカードにその取引を認めるための暗号信号を記録しておき、取引

を行うときに認証ＩＣカードの携帯者が真正な所持者であることを確認して取引を認める仕組みである。

したがって、サービス等の提供者が認証ＩＣカードから受け取るべき情報は、認証ＩＣカードの携帯者がカードの真正な所有者であることと認証ＩＣカードに利用資格を有する証拠となる暗号信号が記録されていることである。また、認証ＩＣカードが認証することは、読み取り装置が適正なものであることと携帯者が真正な所持者であることである。

本発明の認証ＩＣカードでは、建物への入場やある資料室への入室の資格、銀行の口座、クレジットの所有、さらに戸籍、履歴や、電子マネーとして利用する場合の与信残高などを含め、いわば所持者の属性を認証ＩＣカードに収納することにより、利用資格が与えられた全ての取引の認証を１枚のカードに統合することができる。

すなわち、本発明の認証ＩＣカードは、取引資格をカードに与えるのではなくカードの所有者個人に与えるものであるから、従来のカードシステムより本来の信認目的に沿った運用を行うことができる。したがって、従来のようにサービス毎に支給されたカードを多数携帯している必要がなく、従来の多人数で共有する解錠用カードのようにカード自体を他人が利用しないように厳重に管理する必要もない。

本発明の認証ＩＣカードでは、ＩＣカードに記録された情報とカード所有者本人が入力する情報のみに基づいて認証を行うことができるようになっている。したがって、カードのセキュリティはこれまでにも増して重要になるので、真正な取引対象者の署名、声紋、指紋、掌紋、虹彩などの生物学的情報や自由度の大きい暗証番号などを利用して、真正な取引対象者以外の者が認証カードの利用をできないようにする高度な安全確保手段が準備されており、正当利用者でない他人が窃取や拾得などにより取得した認証ＩＣカードを直接利用したり改竄して利用することができない。

しかし、人証情報を忘れた場合に備えて本人には記録した人証情報を教える手段を用意し、また自身の都合により人証情報の書き換えを認めることが必要になるので、こうした手段を利用して本人以外の者が係員を編したり係員と結託して

不正に入手した人証情報を悪用することもあり得る。

また、不正に取得した人証情報を使ってＩＣカードを書き換えたり、あるいは新しいＩＣカードを使って他人の認証カードを偽造するような犯罪行為を完全に防止することはできない。

このように、安全性を高めた認証ＩＣカードでも、使用システムに暁通した者や内部の者が悪意をもって改竄や偽造することまで防ぐことは困難であった。

そこでさらに、本発明の認証ＩＣカードは、ＣＰＵと、人証情報あるいは人証情報と認証情報を格納した認証ファイルと、認証の深さに応じて分類されたジョブプログラムやデータを格納したアプリケーションファイルとを備え、外部からアプリケーションファイルへのアクセスの要求があったときに、認証ファイルの人証情報または認証情報に基づいて真偽を判定した結果によりアクセスを認める認証ＩＣカードであって、認証ファイルに正当利用者自身の人証情報に加えて第２人物の人証情報あるいは主体の認証情報を格納し、第２人物あるいは主体の認証を要求するジョブあるいはデータを予め指定してあって、このような指定のジョブあるいはデータについて実行あるいは提示の要求があったときには、外部から入力される人証情報や認証情報を認証ファイルの人証情報や認証情報と対比して認証に合格したときにＣＰＵを介して指定のジョブの実行やデータの提示を認めるようにしたことを特徴とする。

本発明の認証ＩＣカードによれば、指定したジョブやデータにアクセスするためには、認証ＩＣカードの正当使用者に加えて特定の権限を有する第２人物あるいは主体（以下、立会人という）の承認が必要になるため、特に認証ＩＣカード自体の正当性や使用者の正当性についての確認が重要な問題となるようなジョブなどを指定しておけば、極めて高度なセキュリティを確保することができる。

なお、立会人の承認はＩＣカードに記憶された人証情報あるいは認証情報に基づいて認証されたときに始めて有効になる。

たとえば、認証ＩＣカードを発行するときに１人または２人以上の立会人を立てて、この人物等の人証情報や認証情報を併せて認証ＩＣカードに記録して使用するようにすることができる。このようなカードを使用し、たとえ使用者の要求があってもこの立会人の承認がない限り、一旦入力された本人人証情報を再度見

ることができないようにしたり人証情報や認証情報の書き換えを許さないようにする。なお、立会人は使用者の信認する第三者であってもカード発行責任者の指定する者であってもよい。また、機構や組織としての発行者などの主体であってもよい。

このようなシステムでは、本人でない立会人の承認と認証がなければならず、あるいは本人と立会人が共に揃って認証に合格しなければならないから、窃取者が偽って人証情報の開示を受け認証ＩＣカードを盗用することを防ぐことができるばかりでなく、内部情報に明るい係員が結託して人証情報を書き換えたりすることをも防ぐことができる。

また、認証ＩＣカードの信頼性に基づいて、認証に高いセキュリティを設定することができるため、認証ＩＣカードを発行するカード発行所に特別なセキュリティシステムがなくても認証ＩＣカードの安全性は脅かされることがない。またカードに記憶する個人に関するデータは認証ＩＣカードの中に格納すればよく、認証ＩＣカード発行所に残しておく必要がない。

したがって、信用水準の高いカード発行システムをより容易に構築することができる。

なお、認証の合否判定を行うのは認証ＩＣカード内のＣＰＵであっても、外部装置であってもよい。外部装置を使用する場合は、ＣＰＵを経由して認証ファイルに格納された人証情報または認証情報を外部装置に出力し、外部装置で認証の合否を判定し合格したときに始めて、ＣＰＵを介してアプリケーションファイルへのアクセスを行う。

認証の合否を認証ＩＣカード内のＣＰＵで行うようにした場合は、ＩＣカード読み取り装置側の設備が簡単でよくなり、使用場所における設備費を節約することができる。

また、外部装置で行うときは、ＩＣカードの性能を簡単化することができる。また、人証情報の一部を認証ＩＣカード以外の記憶装置に分担して持たせることにより安全性をさらに向上させるシステムに対する適合性がよい。

なお、人証情報は認証ＩＣカードの真正な所有者の個体を区別する生物学的情報を含むようにすることが好ましい。生物学的情報には、署名、声紋、指紋、掌

紋、虹彩などがある。ただし、生物学的情報以外にも自由度の大きい暗証番号などを利用することも可能であることはいうまでもない。

また。さらに立会人の認証を利用した事項についてのログを認証ＩＣカード内に記録するようにすることが好ましい。

何らかの事故が発生したときに、その状況を把握したり原因を推定するのに役立つからである。

また、本発明のユーザ認証票により認証を行うユーザ認証装置は、ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを取得する人証取得装置と、認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと人証取得装置で取得したユーザの生物学的特徴データを照合して合否を判定する判定装置と、判定結果を出力する表示装置を備えることを特徴とする。

本発明のユーザ認証装置によれば、ユーザ認証票を認証票読取り装置にかけると共に、認証を求められたユーザが人証取得装置を介してユーザ認証票に記録されたものと同じ種類の生物学的特徴データを入力すると、判定装置がユーザ認証票に記録された生物学的特徴データと人証取得装置で取得された生物学的特徴データを照合して合否を判定した結果を表示装置に表示するので、外部と通信をしなくても直ちにユーザ認証票の真正な所有者であるか否かを認知することができる。

なお、ユーザ認証装置にはユーザ登録所に設置される生物学的特徴データ入力装置と同じ種類の人証取得装置を備える必要がある。人証取得装置として手書き図形取り込み機能を有するものを使用することができる。手書き図形取り込み機能を利用して、サインなど予め決めた任意の手書き図形をデジタルデータとして入力すれば、ユーザ認証票の生物学的特徴データと比較することが容易に可能となる。

さらに、本発明のユーザ認証装置は外部の認証局と通信できる通信装置を備え、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し合否の判定結果を受け取り、表示装置を介して判定結果を表示するようになっていることが好ましい。

外部の認証局と接続して認証データを階層的に扱うことにより、悪意を持つ侵害者のアクセスや改竄を防止し、より安全性の高い認証能力を備えることが可能となる。

本発明のユーザ認証システムは錠前管理システムに適用することができる。本発明の錠前管理システムは、利用者の本人認証データを記録したＩＣカードを鍵として用い、入力された人証データとＩＣカードに記録された本人認証データを照合して認証に合格したときに解錠することを特徴とする。

本発明の錠前管理システムでは、錠前の使用を認めた者の本人認証データをＩＣカードに格納したユーザ認証票を鍵カードとして使用者に与える。錠前を解錠するときには鍵カードを提示すると共に人証データを入力する。この人証データを鍵カードに記録されたデータと照合して許容範囲内で合致しているときに始めて錠前を開ける。

アクセスしようとする者の人証データが記録された本人データと合致していなければ錠前を開けることができないから、錠前は認可を受けた者にしか解錠することができない。

このようなシステムは、認定を受けた個人に解錠する権限を与え、その資格を有する本人であるか否かを鍵カードで認証するものであって、鍵カードは鍵機能の一部を担うに過ぎない。

したがって、他人が鍵カードを拾得、盗取あるいは複製して使用しても、本人でない限り錠前を開けることができないため、錠前の安全性は極めて高い。

また、本人情報は鍵カードに格納されているので、錠前装置側に利用予定者全員に関する情報を格納した大量のデータベースを備える必要も、ホスト装置から高速通信により取り寄せる必要もない。

ただし、本人情報の一部を錠前側の記憶装置に格納して、両者を併せて用いるようにすれば、より高い安全を確保することができることは言うまでもない。

なお、鍵カードに記録される本人認証データとして、利用者が所有する生体情報データもしくは利用者が作成する情報データを使用することにより、錠前の安全性はより高くなる。

さらに、鍵カードに記録できる本人認証データの種類が複数あって、選択して

記録できるようにしてもよい。

鍵ＩＣカードを他人が盗用しようとしても、鍵カードが扱う認証データの種類を特定できないようになっていれば、指紋、声紋、署名、暗号などのいずれを使用しているかを知らなければ使えないのでカードを盗んでも役に立たず、盗難カードでの被害も減少する。

また、複数の本人認証データ種類に対応する人証データの入力手段を錠前の利用場所に設置しておいて、利用者が選択できるようにしてもよい。このように複数の認証データ種類が利用できる場合は、盗用者はどの種類の認証データを使っているかを知る必要があり、安全性の高い錠前が得られる。勿論、複数の情報を併用していずれについても合格しなければ解錠できないようにしてもよい。

なお、１枚の鍵カードにより解錠できる錠前が複数あって、それぞれについて適用する本人認証データの種類を選択することができるようにしてもよい。

錠前毎に鍵カードを発行するよりコストが低減すると共に、利用者が携帯するカードの数を節減しかつ錠前毎に対応するカードを選んで提示する煩わしさを省くことができる。

このような鍵カードは、さらに、たとえば保管庫で入口の錠と庫内の仕訳棚の錠を共用する場合などに有用である。保管庫内に管理水準の異なる通常薬品の戸棚と劇薬戸棚を設置しであるときに、保管庫の扉を開ける権限だけでは劇薬戸棚を開けられないようにすることができる。保管庫内に人事情報と経理情報を共に収納してあるがそれぞれ関係者のみしかアクセスできないようにするというような場合にも利用することができる。

なお、このような状況では有資格者以外のアクセスがあった場合に警報する機能を付属すると安全性が向上する。このため、庫内の戸棚に人のアクセスを検知するセンサを設けることができる。センサは有資格者がアクセスする場合は作動する必要がないから、認証を合格した管理区分におけるセンサ回路については警報出力を禁止するようにしておく。

無資格者がアクセスした場合は管理室に警報すると共に、保管庫の扉を閉じてそのアクセス者の逃亡を防ぐように構成しても良い。

また、本発明の錠前管理システムでは錠前にアクセスした者を個人として認識

する機能を有するので、その情報を集積することにより保管庫の利用状況記録を自動的に作製することができる。

本発明の錠前管理システムは、貴重品を保管する金庫に設けて安全を図ることができる。特に貸金庫に利用することにより、管理者側の立ち会いがなくても十分安全な貸金庫設備となる。また、貸金庫利用者自身が、収納物の貴重度に応じてセキュリティの深度を決めてそれに応じた利用をすることも可能である。

図面の簡単な説明

第１図は本発明の実施例のユーザ認証システムを示すブロック図、第２図は本実施例に用いられるユーザ認証装置の例を示す斜視図、第３図は本実施例におけるユーザ認証装置の回路ブロック図、第４図は本実施例に使用するユーザ認証票の第１および第２の構成例を示すブロック図、第５図は本実施例におけるユーザ認証票を発行する手順例を示す流れ図、第６図は本実施例における利用所における認証の手順例を示す流れ図、第７図は本発明の認証ＩＣカードの第３の実施例の構成を示すブロック図、第８図は第３実施例の認証ＩＣカードにおけるファイル構成を示すブロック図、第９図は第３実施例の認証ＩＣカードの使用例を示すブロック図、第１０図は第３実施例の認証ＩＣカードの使用例を示す流れ図、第１１図は本発明の認証ＩＣカードの第４の実施例の構成を示すブロック図、第１２図は第４実施例の認証ＩＣカード発行の手順を示す流れ図、第１３図は第４実施例の認証ＩＣカードに記録した人証情報読み出しの手順を示す流れ図、第１４図は第４実施例の認証ＩＣカードの人証情報書き換えの手順を示す流れ図、第１５図は本発明の錠前管理システムの第１実施例を示すブロック図、第１６図は本発明の錠前管理システムの第２実施例を示すブロック図である。

発明を実施するための最良の形態

本発明の実施形態を添付の図面に従って説明する。

本発明のユーザ認証システムは、第１図にあるように、認定登録局、認証局および認証利用所からなる階層構造を有する。

認定登録局（ＰＲＡ）１は認証ネットワーク全体を統括するもので、ライセン

シーとしての複数の中間認証局（ＰＣＡ）２に一部の権限を与える証明書を発行し、権限を授けられた中間認証局がサブライセンシーとしての複数の末端認証局（ＣＡ）３に一部の権限を与える証明書を発行する。

末端認証局（ＣＡ）３が、ユーザ認証を利用するクライアントとなる認証利用所（ＴＭ）４とクライアントのサービスを利用しようとするユーザ８を仲介する機関となる。なお、以下の説明において各種サービスの利用を取引と表現する場合がある。

なお、認定登録局（ＰＲＡ）１は装置から切り離すことができる記憶装置１１を備え、中間認証局（ＰＣＡ）２と末端認証局（ＣＡ）３は装置に常時接続されている記憶装置２１、３１を備えている。

これらの機関はそれぞれ専用回線や公衆回線により接続されていて、随時情報の交換ができるようになっている。なお、イントラネット網やインターネット網を利用した連結によってもよい。これら通信回線を用いて情報を交換するときは公開鍵や共通鍵を用いた暗号化処理を行うことにより安全を確保するようにすることが好ましい。

なお、中間認証局（ＰＣＡ）はユーザ認証システムを構築する上で省略が可能である。また逆に、中間認証局（ＰＣＡ）を多段に備えて階層の深さが３段より大きくなっていてもよい。

なお、認定登録局（ＰＲＡ）、中間認証局（ＰＣＡ）、末端認証局（ＣＡ）などの機能は相互に合体した機関が実行するようにしても良いことは言うまでもない。

末端認証局（ＣＡ）は、一般には、行政機関、医療機関、特定企業、共同住宅、商店街（モール）など、対象を限った領域についての権限を認定登録局（ＰＲＡ）や上位の認証局（ＰＣＡ）から授与されている。

末端認証局（ＣＡ）３には、この権限を有する領域に属しユーザ認証を利用する認証利用所（ＴＭ）４が接続されている。

認証利用所（ＴＭ）４に該当するものには、役所の各窓口、病院の各科受付や薬局受付、研究所や部課室の扉、保護を必要とするデータベースにアクセスする情報機器、マンション入口や個室の扉、室内ユーティリティの遠隔操作装置、会

員制クラブの施設、モールの各店舗やデパートなど大型小売店の支払窓口、銀行など金融機関の窓口や自動支払機など、各種のものがある。

特にダイレクトマーケティングにおけるユーザ認証は今後さらに重要な課題となり、各ユーザ８の自宅に認証利用所４を設置する状況も考えられる。

末端認証局（ＣＡ）３は、認証利用所（ＴＭ）４を利用しようとするユーザ８を対象として登録の受付をする権限をユーザ登録所（ＲＧ）５に与え、また認証票発行所（ＩＳ）６にユーザ認証票７の発行を行う権限を与える。

ユーザ登録所（ＲＧ）５には、生物学的特徴を取得する入力装置５１が備えられている。本実施例ではタブレットとペンから成るオンライン手書き図形入力装置を利用している。オンライン手書き図形入力装置から筆跡を入力すると、筆記過程の情報を一緒に取り込んで図形認識することができるので、例えば文字を入力したときにも筆画それぞれがどういう方向にどの順序で書かれたかの情報なども容易に取得できる。

また、生物学的特徴をとらえる手段として声紋を利用する場合はマイクロホン５２を装備して音声を入力する。なお、指紋や掌紋を取り込む装置や、瞳を観察して虹彩や網膜パターンを取り込む装置を備えてもよい。

これら人証手段を複数併用することにより、人証をより確実にすることもできる。

認証票発行所（ＩＳ）６には認証票発行装置６１が設置されている。認証票発行装置６１は、ユーザ認証票７に人定に用いられる情報を書き込んでユーザ８に給付する。本実施例におけるユーザ認証システムでは、ユーザ認証票をＩＣカードで構成したが、書き込み読み出し可能な記録媒体であればよく、ＣＤ－ＲＯＭ、フロッピーディスクや磁気カードなど磁気記録媒体、あるいは光磁気記録媒体等、他の電子記録媒体を使用することもできる。

認証利用所（ＴＭ）４には、ユーザ８が持っているユーザ認証票７の真正を検査しユーザ８の認証を行うユーザ認証装置４１が設けられている。

第２図と第３図はユーザ認証装置４１の１構成例を示す図面である。

ユーザ認証装置４１の上面には、認証票７を挿入するスロットがあって挿入された認証票７の記憶領域と情報をやり取りする入出力装置４０１と、取引に要求

BNSDOCID: <WO_____9960485A1_I_>

される認証の深さを指定する認証レベル指定装置４０２と、ユーザの生物学的特徴データを取得する人証入力装置４０３と、認証結果を表示する認証表示装置４０４が配置されている。

なお、人証入力装置４０３は、ユーザ登録所（ＲＧ）５で用いられる生物学的特徴入力装置５１と同じものである。従って、ユーザ認証に声紋を併用する場合には、認証利用所（ＴＭ）４のユーザ認証装置４１にもマイクロホン４２を付設する必要があることはいうまでもない。このように人証入力装置４０３は、利用するユーザの生物学的情報データの種類に従ってそれを取得するために適合する入力装置を備えている。

また、ユーザ認証装置４１の内部には、これら装置を有機的に結合してユーザ認証を行う電子回路４１０が内蔵されている。

この電子回路４１０は、認証票読取り書込み制御装置４１１と人証情報変換装置４１２と判定装置４１３と通信装置４１４から構成されている。

認証票読取り書込み制御装置４１１は、入出力装置４０１を介して認証票の記録内容を読み取り暗号化されたデジタルデータを復号化しまた認証票に取引結果を記憶させる機能を備えている。

また、人証情報変換装置４１２は、人証入力装置４０３で取り込んだ生物学的特徴データをデジタルデータに変換する。

判定装置４１３は、認証票読取り書込み制御装置４１１と人証情報変換装置４１２と認証レベル指定装置４０２の出力情報を取り込み、必要とされる認証レベルに従って通信装置４１４を介して認証局とやり取りした情報を加味してユーザの個人認証を行い、結果を認証表示装置４０４に表示させる。

ユーザ認証が行われて取引が成立すると取引結果が取引内容入力装置４２０から入力され、その内容は取引表示装置４２１に表示されるので、ユーザ８もこれを確認することができる。また、取引の内容は記憶装置４２２に記録される。

なお、判定装置４１３がユーザ認証結果を自動的に取引内容入力装置４２０に送り、取引の受入あるいは拒否ができるようにしてもよい。

さらに、取引内容入力装置４２０から取引情報を入力してユーザ認証票７に取引内容や取引履歴を記録するようにしてもよい。

例えばユーザ認証票７を決済分野に使用する場合は取引目と購入商品名と価額を記録しておけば支払い時における対照確認が容易になる。また行政サービス用の認証票では健康保険証や運転免許証、医療情報あるいは住民基本台帳などの証明書類をユーザ認証票７の中に受領して保存するようにすることもできる。

また、ユーザ認証票７に記録された内容を閲覧するときにユーザ認証を条件とすることにより本人以外のアクセスを排除して、個人のプライバシーを保護することができる。

なお、正しい認証に用いるための生物学的特徴データの他に、特殊な意味合いを持たせた情報を複合して用いるようにしてもよい。例えば、強盗や脅迫者などに脅かされて意志に反してサインをせざるを得ない事態に陥った場合に、正規のサインに何気なく隠し記号を付け加えると、扉の開閉や現金の引出など普通に取引が成立するが、同時に警備会社にも通報が行っていて、利用者の安全が確保された状態になったところで犯人を逮捕するなど、適当な処置を執るようにする仕組みを持たせるようなこともできる。

こうした目的に使用する生物学的特徴データとして、例えばサインすると同時に軽く２回咳払いするなど、異なる種類のものを複合して用いても良い。

第４図は、ＩＣカードを使用したユーザ認証票の内部構成を示すブロック図である。

本実施例で用いられるユーザ認証票７は、複数の発行者が共同で共用端末を設置し相互解放するための便宜を考慮して、接続端子７１を介して電気信号を伝達する接触型と、カード内の電極７３と認証票読取り書込み制御装置内の電極が接触しないで静電結合や電磁誘導などにより通信する非接触型との両方を備えた複合型ＩＣカードを採用するが、いずれか一方の方式を設備したものであってもよい。

接続端子７１には接続回路７２、非接触電極７３には通信制御回路７４が接続されていて、内蔵するメモリーと連結されている。

ユーザ認証票７は、ランダムアクセスメモリＲＡＭ７６と読み出し専用メモリＲＯＭ７７と電気的に書込み可能なプログラム可能読取り専用メモリＰＲＯＭ７８と電気的に消去可能なプログラム可能読取り専用メモリＥＥＰＲＯＭ７９から

なるメモリーとＣＰＵ７５を備えていて、相互間はバスにより接続されている。

接続回路７２と通信制御回路７４とＣＰＵ７５およびメモリーは１個のＩＣチップに収容することができる。

認証票読取り書込み制御装置４１０は、ユーザ認証票７が挿入されると接続端子７１から接続回路７２を介し、または非接触電極７３から通信制御回路７４を介して、ユーザ認証票７のメモリーにアクセスすることができる。

ＰＲＯＭ７８には認証票の真正性を検査するために使用するカード認証データや証明を受けてユーザ認証票を発行した発行者を明らかにするＩＤなどが格納され、一旦書き込んだデータは書き換えることができない。

ＥＥＰＲＯＭ７９にはユーザの認証に用いる生物学的特徴データや認証票を用いた取引の記録が格納される。またＲＯＭ７７にはＣＰＵ７５を制御して、暗号化や復号化、データ入出力の管制、ユーザ認証装置４１の真正性検査などを行うプログラムが格納されている。ＲＡＭ７６は外部から取り込むデータや演算過程で必要となるデータを一時保持する機能を有する。

ユーザ認証票７は認定登録局１で認証システムに使用される適正なカードであることが保証できる正しいカード認定情報をＰＲＯＭ７８に書き込んだ状態で各認証票発行所６に配布されている。従って、認証票発行所６は認定登録局１からの指示に基づいてユーザの生物学的特徴データの一部をＥＥＰＲＯＭ７９に書き込めばよい。カードの改竄を認めないようにするために、認証票発行装置はＰＲＯＭ７８の書き換え機能を備えないようにしても良い。

ただし、本実施例における認証票のメモリー配分は上記に限られず、例えば本人認証を行うための生物学的特徴データをＰＲＯＭ７８あるいはＲＡＭ７６に記録するようにしても良い。

第５図を用いてユーザ認証票を発行する手順の１例を説明する。

ユーザ登録所５は、その管轄領域内の認証使用所４のサービスを受けることを欲するユーザ８から登録申請を受け付ける（Ｓ１１）。この時ユーザ登録所５は必要に応じてユーザ８の資格審査に用いる情報を聴取するとともに、ユーザ個人の生物学的特徴を表す情報を取得する（Ｓ１２）。ここで利用する生物学的特徴はユーザ個体に特有であって、他人が模倣や変装などによりそのユーザになりす

まそうとしても見破ることができるような性質を有するものが選択される。

本実施例では、筆跡を用いて識別するようにしている。入力する図形は任意でよいが、ユーザ８が入力する度に異なるのは認証を行う上で具合が悪いので、普通は、再現性を保証するため自己の氏名を表すサインを入力させるのが好ましい。なお、複数の生物学的特徴を用いると認証の安全性が向上するため、補助的にマイクロホン４２を用いて声紋も取得できるようにしてある。

ユーザ登録所５で採取された申込人の資格情報と生物学的特徴データは認定登録局１に伝送される（Ｓ１３）。

認定登録局１は、ユーザ登録所５から受け取った情報に基づいて資格審査をし、合格した者に対して認証票の発行を許可する（Ｓ１４）。資格条件は認証を利用する対象に従って決まるので、実際にユーザを受入れる末端認証局３で審査するようにしてもよい。

認定登録局１は、登録ユーザ８の生物学的特徴データを所定の割合に従って階層的に分割し、ユーザ認証票７と各段階の認証局２，３に分配する部分を決定して各所に配布する（Ｓ１５）。

認定登録局１で各所に分配された生物学的特徴データは、認証利用所４の要求する認証精度に基づいてアクセスするものであり、最も低度の信頼性で足りる場合は認証利用所４の認証装置４１で対照した結果だけで認証できるようにし、中度の信頼性を要求するときは末端認証局３に格納された情報を加味してユーザ認証し、最も高度の保証を要求する場合は分散格納された全ての生物学的特徴データを統合して判定するようにする。

本発明のユーザ認証システムでは、生物学的特徴データは初めに認証利用所４で真正性を検査して合格したときだけ上位機関の認証を請求できるように構成する。上位の認証機関ではユーザ認証票にない部分の情報を用いた認証を行う。

従って、ユーザ認証票７には最小限ユーザ８が入力する生物学的特徴データと対比することによりある程度の確度で真正ユーザであることが判断できる情報を配分しておかなければならない。

本実施例では約６０％の情報をユーザ認証票７に分配し、末端認証局３に３０％の情報、中間認証局２に残りの１０％の情報を分配することとした。このよう

BNSDOCID: <WO 9960485A1_I_>

に級数的に情報量を減少させることで、より多数の認証請求が集まる上位機関の記憶容量を節約し、かつ認証に要する時間負荷を減少させる効果が生じ、システム全体としての情報保護性能の向上を図ることができる。

なお、より高度な保証を要請されたときに上位の機関に送達する情報が過大にならないためには、ユーザ認証票７に保持する生物学的特徴データの割合がある程度大きい方が好ましい。

しかし、ユーザ認証票７に与える情報の比率が過大になるとユーザ認証の信頼性が低下する。

従って、生物学的特徴データの分配に当たっては、接続するユーザ数や要求される認証の安全性などを勘案し、実際の条件に適合した適切な分割割合を定める必要がある。

情報の分割方法は、デジタル情報化されたデータを所定の割合で物理的に分割する方法であってもよいが、また筆跡のように描き終わった形状に関する情報と描いている途中の筆勢に関する情報、さらに筆順などの情報というように段階を追った情報として分割してもよい。例えば、声紋を周波数帯に分割したり指紋を指毎に分けてそれぞれに記録して利用するなど、生物学的特徴は、いずれも適当に分割して利用することができる。

なお、筆跡と声紋など複数の特徴を取得して異なる種類ごとに分割して用いてもよい。

認定登録局１は、認証票とユーザに関する情報を磁気テープやＣＤ－ＲＯＭ、光磁気ディスク、ＤＶＤ、あるいはリムーバブルハードディスクなど、装置から切り離すことができる大容量の記憶手段１１に記録して保存し（Ｓ１６）、下位機関から要請があったときに係員が再生装置に装着して登録された情報を照会するようにする。

認証登録局１では、取り外し可能な記録装置１１を用いて、情報記録媒体１１は不要時には外部の通信回路網から切り離して保管するので、外部からの侵襲や改竄を防止することができる。

認証局２、３に配布された個人の生物学的特徴データはそれぞれに付属する記憶装置２１、３１に格納され必要に応じて随時読み出して利用する。

認証票発行所６は、認証票毎に決められたカード認証暗号が記録されているユーザ認証票７に認定登録局１から分配を受けた登録申込人の生物学的特徴データを記録してユーザ８に支給する（Ｓ１７）。

なお、１個の末端認証局（ＣＡ）３に複数のユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６を備えてもよい。

ユーザ８はユーザ登録所５に出頭して実際に自身の生物学的特徴を入力しなければならないので、発行されたユーザ認証票７を受け取る認証票発行所６がユーザ登録所５と同じ場所に設置されているとユーザ８の便宜のために好ましい。

なお、ユーザ８の人定のため信頼がおける人物の立会を条件とするようにしてもよい。ただし、初めから他人になりすましている場合を完全に排除することはどの様な機構を用いても困難である。

また、登録するユーザが申告した事実を確認するためには、登録手続と同時に認証票を発行する方式でなく、後に住所に郵送する方式を採用してもよい。

なお、認定登録局（ＰＲＡ）１がユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６を備えるようにしてもよい。

さらに、ユーザ登録所（ＲＧ）５と認証票発行所（ＩＳ）６の機能を備えた携帯用端末を持った発行者が任意の場所において登録発行手続をすることも可能である。このような携帯用端末の利用は認定登録局（ＰＲＡ）から正規の資格認定を受けた者しか認めないようにする必要があり、ここでも発行者としての厳重な認証を受けて始めて操作できるように構成されている。

次に、第６図を用いて、認証利用所４においてユーザ認証票７によりユーザ認証をする手順の１例を説明する。

ユーザ８がユーザ認証票７を提出して認証利用所４に取引を申し出ると、認証利用所４はその認証票７を認証装置４１のカードスロット（入出力装置）４０１に挿入して認証用の情報を読み取る。認証用の情報にはカードの真正性を確認するための情報とユーザ認証のための生物学的特徴データとが含まれる。

認証利用所４は初めにカードの認証を行う（Ｓ２１）。カードの認証は、ユーザ認証票７が認証利用所４が使用するユーザ認証システムに適応する真正なものであり正当な所持者が誰であるかを確認することである。対応しない認証票を使

BNSDOCID: <WO 9960485A1 I >

用している場合は初めから取引を受け付けない。

なお、逆にユーザ認証票７が不正にアクセスされていないことを確認するために、ユーザ認証票７中のプログラムにより認証装置４１が自身の認証票と対応するものであるかを検証して、正しい認証装置でない場合は記憶内容の開示を拒絶する仕組みを備えてもよい。

カード認証で合格したときには、ユーザ８にタブレット（人証入力装置）４０３上にサインを書いて貰うなど、ユーザ認証票７を取得したときに用いたものと同じ生物学的特徴を表示することを求める（Ｓ２２）。

そして、タブレット４０３から入力した生物学的特徴データをユーザ認証票７に記録されていた例えば６０％の生物学的特徴データと照合して、窓口のユーザ８がユーザ認証票７の真正な所持者か否かを判定する（Ｓ２３）。ユーザ認証結果は表示装置４０４に表示する（Ｓ２４）。

認証利用所４におけるユーザ認証の合否に従い手順が異なる（Ｓ２５）。ユーザ認証が否定されたときは認証利用所４は取引を拒絶する（Ｓ３３）。ユーザ認証に合格したときはさらに上位の認証機関にオンライン認証を求めるべきか否かを調べる（Ｓ２６）。オンライン認証を必要としない場合は直ちに取引の申し出を受け入れてよい（Ｓ３２）。

オンライン認証の要求の有無や深さの要求度は取引毎に認証レベル指定装置４０２からオペレータやユーザ８が入力してもよいが、取引の性格や取引金額の多寡に基づいて自動的に設定されるようにしてもよい。

オンライン認証を必要とする場合は、認証レベルの要求と共にユーザ認証票７の情報と人証入力装置４０３で取得した人証情報とを末端認証局３に送付する（Ｓ２７）。送付する人証情報は、認証利用所４で利用した部分を除外した例えば４０％の部分でよいから、認証利用所４と末端認証局３の間で交換する情報量を縮減することができる。

オンライン認証の要否は、取引の性格に従った認証の安全性に対する要求水準により決められる。換金性の高い商品や高額商品の取引とか個人の秘密情報の開示にはより安全な認証が必要とされるので、上位機関のユーザ認証が求められることになる。

また、認証利用所４の性格によってオンライン認証の深さが指定される場合もある。病院の窓口などではプライバシーの保護と正確な治療行為を保証するため高度な本人認証が必要とされる場合が多い。なお、通信回線を使った在宅診療などでは確実に本人のデータであることを確認するため、上位の認証局までユーザ認証を求めるようにすることが好ましい。

末端認証局３では記憶装置３１に記録されているユーザ８の固有の人証情報と照合して（Ｓ２８）、認証結果を認証利用所４に回付する（Ｓ２９）。

末端認証局３にはユーザの人証情報の３０％しか記録されていないので、ここにおけるユーザ認証だけでは不足する場合は、さらに上位の中間認証局２にユーザ認証を求める。中間認証局２には各ユーザについて１０％の生物学的特徴データを記録してあるので、認証利用所４で取得した人証情報のうち中間認証局２で使用する部分は１０％になり、末端認証局３から中間認証局２に送付すべき情報量はさらに大幅に減少する。

中間認証局２で行ったユーザ認証結果は末端認証局３を介して認証利用所４に返る。

各所のユーザ認証結果は認証利用所４で総合されてユーザ認証装置４１の認証表示装置４０４に表示される。ユーザ認証が合格の場合は取引を受け入れ（Ｓ３２）、不合格の場合は取引を拒否（Ｓ３３）することになる（Ｓ３１）。

また、ユーザ認証が否定されたときは改竄やなりすましなど何らかの不正行為の可能性もあるので、その情報を認定登録局１まで送付して問題の在処を確認して原因の解析を行うことが好ましい。

認定登録局１には外部から侵入したり改竄することが困難な記録が保管されているので、認証利用所４における入力データと対比することにより、異常がユーザ認証票７にあるのか、末端認証局３にあるのか、あるいは中間認証局２にあるのかが明確になる。

ユーザ認証票７の内容とユーザ８が入力した情報の間に齟齬がある場合は盗難や拾得により真正でないユーザが使用している場合やユーザ認証票のデータが不当なアクセスにより書き替えられた場合が考えられる。

次に、本発明のユーザ認証システムの第２の実施例について説明する。

本実施例のユーザ認証システムが第１の実施例と異なる点は、認証利用所に設けた論理演算装置でユーザ認証票に記録した生物学的特徴データと人証取得装置で入力させたユーザの生物学的特徴データとを対照して行う代わりに、ユーザ認証票内の演算機能によりユーザの生物学的特徴データと記録された人証情報とを対照するようにした点のみであるので、ここでは、第１実施例の説明に使用した図面を用いて第１実施例と異なる部分についてのみ説明する。

ユーザ認証票７として使用するＩＣカードには、ＣＰＵ７５やＲＡＭ７６などを搭載して一定の演算機能を持たせることができる。

本実施例のシステムでは、認証利用所４でサービスを利用しようとするユーザ８がユーザ認証装置４１を用いてユーザの生物学的情報データを入力すると、この生物学的情報データを所定の処理をしてデジタル処理しやすい形態に変換した上でユーザ認証票７に送付する。

ユーザ認証票７は入力された情報データを一旦ＲＡＭ７６に記憶し、ＣＰＵ７５でこの情報データとＥＥＰＲＯＭ７９に記録されている正当ユーザの生物学的情報データを読み出しながら両者を突き合わせて比較する。その結果、両者が許容範囲内で類似していてサービスを利用しようとする人間がユーザ認証票７の正当な所有者ということが認証できれば認証利用所４に合格を通知し、この認証にパスしなければ拒絶を通知する。

認証利用所４は、ユーザ認証票７のユーザ認証結果に満足すれば利用者８に所望のサービスを提供する。また、さらに慎重なユーザ認証を必要とする場合は末端認証局３や中間認証局２に照会を行って、その結果と合わせて判定する。なお、認証利用所４が末端認証局３を兼ねていても良いことは言うまでもない。

各所に生物学的情報データを配布する割合は任意であるが、第１実施例で例示したと同様に下位水準の認証に用いるものほど大きな割合にすると通信における負担が軽くなりシステムの運用上有利で、ユーザ認証票７における割合を６０％以上にすることが好ましい。

本実施例では、高機能ＩＣカードからなるユーザ認証票７を活用することによりユーザ認証装置４１の演算上の負担を軽減し装置のコストを低減できることから、認証利用所４の機能を調えるのに必要とされる費用が小さくなるので、シス

テムに参加するための障壁が低くなりより利用しやすくすることができる。

また、ユーザ認証票内で情報処理を完結させるので、認証票のメモリに外部からアクセスできない読み出し不可領域を設けて、ここに認証データなど重要な情報を記録して漏洩を防ぐようにして安全性をより向上させることができる。

本発明のユーザ認証システムに使用するユーザ認証票の第３の実施例は、第７図に示したようなＩＣカードを用いた認証ＩＣカードで、要求されるレベルの認証に合格したときにＩＣカードに格納された情報を利用に供するようにしたものである。認証ＩＣカードに認証情報を１００％格納するようにして、上位の認証局を利用しないようにしてもよい。

この実施例の認証ＩＣカードは、情報処理を実行するＣＰＵ１０１、情報処理プログラムを収納したＲＯＭ１０２、演算用データを記憶するＲＡＭ１０３、情報の書き込み読み出しが可能なデータ記憶装置１０４、アプレットプログラムに対するインターフェース１０５、外部接続用接続回路１０６、および外部接続端子１０７を備える。

データ記憶装置１０４のファイルには、第８図に示したように、認証データを記憶した認証ファイル１１０と、外部とやり取りする情報を格納したアプリケーションファイル１２０が含まれる。

なお、外部接続端子１０７は、信号伝達および電源の供給に用いられるが、非接触型の電極やアンテナであっても良い。また、各種のカード読み込み装置に対応するため接触型と非接触型の両方の接続端子を備えるようにしても良い。

アプレットインターフェース１０５は、外部から小型プログラム（アプレット）を受け入れてそのプログラムに従ってＣＰＵを作動させる場合に用いるもので、受け取ったアプレットが認証ＩＣカードにとって無害であることを認識する機能を備えたインターフェースである。

安全のため認証ＩＣカードがアプレットを受け付けないようにしてもよく、このような認証ＩＣカードではアプレットインターフェース１０５も無用である。

認証ファイル１１０には、認証ＩＣカードが真正であることを保証するためのデータに加えて、認証ＩＣカードの真正な所有者を認証するための人証情報が格納されている。認証は簡単なものから高度な保証を与えることができるものまで

段階Ⅰ，Ⅱ，Ⅲ，…を追って複数のものが記録されている。人証情報は、たとえば暗証番号、指紋、声紋、顔写真、サイン筆跡など、本人しか知らないものや生物学的情報で本人以外では再現できないようなものが好ましい。

アプリケーションファイル１２０は、格納する情報の種類に関する第１の分類と認証に関する第２の分類にしたがって区分されている。すなわち第１分類ａ，ｂ，ｃ，…は、例えば住宅管理用情報、医療情報、金融情報、通信情報など、通常は認証を使用するサービス機関を区別するために使用される分類である。第２分類Ⅰ，Ⅱ，Ⅲ，…は、要求される認証の程度に従った分類で、簡単な認証でアクセスを認めるものから、指紋で確認するなど高度な認証に合格して始めてアクセスを認めるものまで認証深さにより分類されたものである。

たとえば、ビル管理会社から提供される情報を格納するのは第１分類ｂで、住宅棟の入場許可暗号はその第２分類Ⅰのファイルに、クローゼットの開扉暗号は第２分類Ⅱのファイルに、また自室の扉の開扉暗号は第２分類Ⅲのファイルに記録されている。

なお、これらのファイルには暗号の鍵や電子証明書などを入れておくこともできる。

住宅棟の入口にはカード読み取り器が設備されていて、入居者が認証ＩＣカードを読み取り器に読み込ませると、カードと読み取り器の間で相互に真正性をチェックして合格すると扉が開き住宅棟に入ることができる。住宅棟内の各室には厳重な扉が付いているため、単に認証ＩＣカードが真正であることを確認するだけの簡単な認証で住宅棟への立ち入りを許可している。

なお、認証ＩＣカードがカード読み取り器が真正なものであることを確認する機能を持つのは、真正でないカード読み取り器で認証ＩＣカードに格納されている情報を窃取したり内容の書き換えをすることを防ぐ必要があるからである。

第９図は、認証ＩＣカードの利用方法の代表的な例として住宅の管理に使用した例を挙げて説明したブロック図である。

各室の扉３０には扉開閉制御装置１３１が設備されていて、扉１３０は通常手で開けることができないようになっている。扉開閉制御装置１３１には認証制御装置１３２が接続されていてここから発生される制御信号に従って扉の開閉が行

われる。認証制御装置１３２には人証情報入力装置１３３とカード読み込み器１３４が接続されている。

以下、第１０図の流れ図を参照しながら、認証ＩＣカードを使用するときの情報処理手順を説明する。

入室しようとするカード使用者が認証ＩＣカード１３５をカード読み取り器１３４に挿入すると（Ｓ４１）、認証制御装置１３２は読み取り器ＩＤを認証ＩＣカード１３５に送ると共に認証ＩＣカードのＩＤを問い合わせる（Ｓ４２）。認証ＩＣカード１３５は読み取り器ＩＤを認証ファイルの情報と対照して検査し、自己のカードを扱って良いものであることが確認できたときに（Ｓ４３）、認証ファイルに記録されているカードのＩＤをカード読み取り器１３４に返送する（Ｓ４４）。これらのやり取りは全てＣＰＵを介して行われ、カード読み取り器１３４は直接的に認証ＩＣカードの記憶装置にアクセスできない。

認証制御装置１３２は認証ＩＣカードのＩＤがシステムに適合した真正なものか否かを判断し（Ｓ４５）、適合しない場合はカードを排出して拒絶する（Ｓ５０）。適合している場合には、認証レベルに基づいて決められた例えば指紋など、人証の入力を督促し、使用者が人証情報入力装置１３３から入力する情報を読み取り（Ｓ４６）、入力した情報を抽出処理して人証情報を作成する（Ｓ４７）。

人証情報が真正か否かを認証ＩＣカード側で確認するか扉開閉制御装置側で確認するかを判定し（Ｓ４８）、認証ＩＣカード１３５で確認することになっている場合は、人証情報を認証ＩＣカード１３５に伝達すると共に扉を開くための開扉暗号を求める（Ｓ４９）。

認証ＩＣカード１３５は受け取った人証情報を認証ファイルに格納されている人証情報と照合して（Ｓ５０）、両者が合致すると認められる場合は、所定のアプリケーションファイル（例えばｂⅢのファイル）に記録されている開扉暗号をカード読み取り器１３４を介して認証制御装置１３２に送付する（Ｓ５１）。

なお、人証情報が真正か否かを扉開閉制御装置側で確認する場合は、認証ＩＣカード１３５に対し記録されている人証情報を要求し（Ｓ５２）、認証ＩＣカード１３５が回答してきた（Ｓ５３）人証情報と先に取得したカード使用者の人証情報との照合を行い（Ｓ５４）、合格したら今度は認証ＩＣカード１３５に対し

BNSDOCID: <WO_____9960485A1_I_>

開扉暗号を求める（Ｓ５５）。認証ＩＣカード１３５は求めに応じて所定のアプリケーションファイルに記録されている開扉暗号を認証制御装置１３２に送付する（Ｓ５１）。

こうして受け取った開扉暗号が真正であれば（Ｓ５６）、扉開閉制御装置１３１に開扉指示信号を与えて（Ｓ５７）扉１３０の解錠をするので（Ｓ５８）、認証ＩＣカードの所持者が入室することができる（Ｓ５９）。

また、認証ＩＣカード１３５のデータ記憶装置１０４の使用領域を少なくするために人証情報を分割して認証ＩＣカード１３５と認証制御装置１３２に分納することもできる。この場合は人証入力装置から入力された人証情報と認証ＩＣカード１３５と認証制御装置１３２とに分割されて格納されている人証情報とを照合して開扉暗号を出す。このように人証情報を認証ＩＣカード１３５と認証制御装置１３２とに分割することは、単にメモリ領域の節約だけでなく、仮に認証ＩＣカードの認証ファイルから人証情報が盗まれたとしてもそれだけからでは照合することができないため、セキュリティ面での効果もある。

また、上記の例では、認証ファイルに格納される人証情報として３段階使用したが、段階の数はいくつに設定しても良い。人証情報としては、カードの発行者が記入しておくＩＤ番号のみに基づいて真正を証明する最も簡単な段階から、カードの所有者が決めた暗証番号、所有者の指紋、虹彩、顔写真などの生体情報、所有者が入力するサインなどの動的情報、さらにこれらを組み合わせたより高度な複合情報などが使用できる。

なお、生体情報は真正な所持者の身体が生物学的に所有している情報で真似することが困難ではあるが、情報をコピーすることにより成り澄ますことができる。これに対し、現場における本人の動作を伴う動的情報を利用すると成り澄ましが困難になるので、より信頼性の高い認証ができる。

人証情報入力装置は、サイン入力を要求する場合は図形入力装置、暗証番号を使用するときにはキーボード、指紋を使用するためには指紋取得装置、虹彩を利用する場合は瞳を撮像するカメラと判定装置など、使用する人証情報に応じて、その情報を取得する装置を準備しなければならない。

また、ＩＣカードに記録された個人的情報をアクセスする場合や、病院でカル

テを開示させる場合のように、所持者が認証の深さを指定することが好ましいことがある。例えば住民票を取るときと納税証明書を取るときで認証の深さを変えたいと思えば、それぞれの証明を求めるときに使用する暗号番号を格納するアプリケーションファイルの認証深さの指定を変えればよい。

医療における支払いをするときと通信網を利用した在宅診療を受けるときでは、本人認証の重要性が異なることは明らかであるが、このような場合にも本発明の認証ＩＣカードは的確に対応することができる。

なお、１枚の認証ＩＣカードを会員証や社員証、あるいは行政窓口における本人証明カードとして利用したり、交通機関の定期券、プリペイドカード、クレジットカード、テレホンカード、ショッピングカード、あるいは与信残高金額を書き換えることができる電子マネーとして使用することもできる。

また、ホテルなどでチェックイン時に部屋の扉開閉を行う暗号を認証ＩＣカードのファイルに記憶しチェックアウト時に消去するというように、一時的な利用も可能である。

本発明のユーザ認証システムに使用するユーザ認証票の第４の実施例は、第１１図にあるような認証ＩＣカードで、保証人や立会人の認証を追加したところに特徴がある。

本実施例の認証ＩＣカードは、第３実施例の認証ＩＣカードと同様、演算処理を実行するＣＰＵ２０１、演算処理プログラムを収納したＲＯＭ２０２、演算処理中のデータを記憶するＲＡＭ２０３、データの書き込み読み出しが可能なデータ記憶装置２０４、アプレットプログラムに対するインターフェース２０５、外部接続用接続回路２０６、および外部接続端子２０７を備える。

データ記憶装置２０４のファイルには、認証データを記憶した認証ファイル２１０と、特定のジョブを実行するためのジョブプログラムや各種データを格納したアプリケーションファイル２２０が含まれる。

認証ファイル２１０には、認証ＩＣカードが真正であることを保証するためのデータや、真正な所有者の人証情報が格納されている。認証情報は１種に限らず多数種類格納しておいて１個単独でもしくは複数個を複合して使用することができる。

BNSDOCID: <WO_____9960485A1_I_>

認証ファイル２１０には、認証ＩＣカードにより認証する真正な所有者の人証情報を記憶した第１人証ファイル２１１と、保証人や立会人あるいは発行人などの第２の人物に関する人証情報や主体に関する認証情報を記憶する第２人証ファイル２１２とが含まれている。これら第２人物や主体などの立会人はシステム上の必要に応じて２人以上の人物や主体であってもよい。

アプリケーションファイル２２０は、認証ＩＣカードの真正性に関する情報を扱う部分が格納された第１作業ファイル２２１と、認証結果に基づいて実行するための部分が格納されている第２作業ファイル２２２を含む。

第２作業ファイル２２２には、認証を使用するサービス機関毎に必要とされる情報が、要求される認証の程度に従って分類された状態で格納されている。なお、暗号の鍵や電子証明書などを入れておくこともできる。また、開錠指示を発するジョブなどのプログラム類を格納しておいてもよい。

また、第１作業ファイル２２１には、人証情報を書き込むジョブや、人証情報の読み出しや書き換えを行うジョブ、あるいはログの読み出しや消去を行うジョブなど、認証ＩＣカードの真正性に係わるジョブや情報が格納されている。

第１作業ファイル２２１に格納したジョブや情報は、要求される機密水準に基づいて、所有者のみ認証すればよいものと、第２人物のみ認証すればよいものと、所有者と第２人物の両方を認証しなければならないものとに分けておくことができる。

次に、第１２図から第１４図を参照して本実施例の認証ＩＣカードの使用例を説明する。

第１２図は、認証ＩＣカードを発行するときの手順を例示するものである。

認証ＩＣカードの発行要求があると（Ｓ１１１）、カードの発行者は認証カードの認証対象者の信用審査をし（Ｓ１１２）、この審査に合格して認証対象者が認証カードを正当に使用できる者であると認定できるときは、認証対象者の保証ができる人あるいは認証対象者が信頼する人を立会人として指名させる（Ｓ１１３）。

認証ＩＣカードを発行するときには、指定のカード発行所に関係者全員が集合して（Ｓ１１４）、認証ＩＣカードとカード発行装置が互いに真正であるかを確

認して（Ｓ１１５）、認証ＩＣカードの発行を認めると（Ｓ１１６）、各人が人証情報を入力する（Ｓ１１７）。

なお、認証ＩＣカードにカード読み取り器が真正なものであることを確認する機能を持たせるのは、認証ＩＣカードに格納されている情報を窃取したり内容の書き換えをすることを防ぐ必要があるからである。

カード所有者になる人は、カードに基づいて取り引きするときに取引に要求される信用度が異なることに対応して、暗証番号、独自の記号、サイン、指紋、声紋、虹彩、掌紋など幾つかの人証情報を入力する。立会人についても複数の人証情報を入力させてもよいが、立会人の認証が必要となるケースは限られているので、幾つもの人証情報を使用する必然性はない。なお、立会人は組織や機構としての主体であってもよく、この場合には生物学的情報の代わりに電子サインのような認証情報により認証を行うようにすることができる。

なお、認証ＩＣカードは社内で種々の権限を確認するために使用する場合もあるが、このような場合に例えば発行を担当する人事部などの部局の責任者や発行担当係員が上記カード発行者や立会人として認証を受けるようにしてもよい。あるいはカードを所持する人物の属する部局の責任者が認証を受けるようにしてもよい。

入力された所有者本人の人証情報は認証ＩＣカード中の第１人証ファイル２１１に格納し、立会人等の人証情報や認証情報は第２人証ファイル２１２に格納する。また、認証を行ったときにその認証の信頼性や根拠を記載した電子証明書を要求されることがあるが、このような認証ＩＣカードが発行することになる電子証明書は各種の取引類に用いられるアプリケーションデータと共にアプリケーションファイル２２０中の第２作業ファイル２２２に格納される（Ｓ１１８）。

なお、認証ＩＣカードに記録された人証情報を表示させたり書き換えを行うためのプログラムは第１作業ファイル２２１に格納されており、アクセスするためにはそれぞれのジョブに対応して予め決められた認証を満足しなければならない。

上記のように、必要な情報を書き込んだ認証ＩＣカードは、認証対象者が適正な人証情報を入力したときに適正な動作をすることなど、製品としての完成度を確認する適当なテストを受け（Ｓ１１９）、これに合格すると所有者に交付され

BNSDOCID: <WO_____9960485A1_I_>

る（Ｓ１２０）。合格しない場合は、例えば認証情報等の書き込み工程（Ｓ１１８）をやり直して適正な認証ＩＣカードにしてから交付する。

なお、発行主体の審査により（Ｓ１１２）カードの認証対象者がカードにより認証システムを利用するのに相応しくないと判定したときは認証ＩＣカードの発行は拒絶されることになる（Ｓ１２１）。

このような認証ＩＣカードは、サービスや取引（代表して取引と呼ぶ）毎に利用資格を与えられた者が所持する認証ＩＣカードにその取引を認めるための暗号信号を記録しておき、取引を行うときに認証ＩＣカードの携帯者が真正な所持者であることを確認して取引を認める仕組みに用いることができる。

この場合に、取引者が認証ＩＣカードから受け取るべき情報は、認証ＩＣカードの携帯者がカードの真正な所有者であることと認証ＩＣカードに利用資格を有する証拠となる暗号信号が記録されていることである。また、認証ＩＣカードが認証することは、読み取り装置が適正なものであることと携帯者が真正な所持者であることである。

この認証ＩＣカードでは、建物への入場やある資料室への入室の資格、銀行の口座、クレジットの所有、さらに戸籍、履歴や、電子マネーとして利用する場合の与信残高などを含め、いわば所持者の属性を認証ＩＣカードに収納することにより、利用資格が与えられた全ての取引の認証を１枚のカードに統合することができる。

このような認証ＩＣカードは、第３実施例におけると全く同じように住宅の入室管理などに使用することができ、他人による成り澄ましが困難な信頼性の高い認証ができる。

この認証ＩＣカードは多種類の人証情報を場合によって使い分けるようになっている。そこで、真正な所有者といえども自分が使用すべき人証情報を忘れてしまうことが間々ある。このような場合に、カードが使用できなくなるのでは不便なので記録された人証情報を表示できるようにするのが普通である。

また、人証情報は他人に漏れて盗用されそうなときや安全性を高めるために定期的に変更するときなど、所有者本人の必要により変更できるようにしておくことが好ましい。

したがって、認証ＩＣカードの構造に詳しく取り扱い機器を自由にすることができる人物が悪意を持って認証ＩＣカードに格納した情報を引き出して、カードを改竄したり、偽の認証ＩＣカードの作製を行おうとすれば、これを防止することは容易でない。

ところが、本実施例の認証ＩＣカードは予め決められたジョブについては立会人の認証を求めることができるから、認証ＩＣカードの認証情報にアクセスする場合には立会人の承認を要求することにしておけば、内部事情に詳しい者であっても人証情報を盗み出して利用したり人証情報を書き直したりすることができない。

第１３図は、真正な認証対象者が自己の人証情報を確認するときに要求される手順を示す流れ図である。

認証ＩＣカードの人証情報を読み出したいときは（Ｓ１３１）、カードにより認証を受けるべき認証対象者とカード発行時の立会人とカード発行所の責任者あるいは組織としての主体が集合して（Ｓ１３２）、カードが真正なものであるかを確認の上（Ｓ１３３）、それぞれ人証情報あるいは認証情報を入力する（Ｓ１３４）。

それぞれの人物等の人証情報・認証情報を認証ＩＣカードに格納されている人証情報・認証情報と参照して一致していれば（Ｓ１３５）、このようなアクセスがあったという事実を認証ＩＣカード内の記憶装置にログとして残し（Ｓ１３６）、記録されていた人証情報をカード読み込み装置に付属するディスプレーに表示する（Ｓ１３７）。必要な人証情報等が一致しない場合は不正なアクセスであるので、人証情報の表示を拒絶する（Ｓ１３８）。

なお、カードの認証対象者は覚えている人証情報をひとつ入力し、これが認証ＩＣカードに格納されているもののひとつに一致していればよいとする。ここで、たとえば暗証番号を忘れたときは指紋の参照で開示するが、サインを知りたい場合には暗証番号が一致しても教えないようにするなど、表示を求める人証情報より高度の人証情報で認証できたときに限って表示するようにしてもよい。

また、高度な安全性を要求しない人証情報については、立会人等が集まらなくても、所有者本人の生物学的特徴に基づいた人証情報により本人認証ができれば

開示するようにしてもよい。なお、特別な場合はカード発行責任者がその責任において独自に情報を読み出せるようにすることも可能である。

第１４図は、人証情報の書き換えを行うときの手順を表す流れ図である。

人証情報の書き換え要求があったときには（Ｓ１４１）、認証対象者本人だけの了承でよしとすると他人による不正使用を排除することができない場合があるので、立会人や発行担当者等を集めて（Ｓ１４２）全員が承認することを確認する。認証ＩＣカードと発行装置の真正性を互いに確認した後（Ｓ１４３）、集合した人物等のそれぞれが人証情報・認証情報を入力する（Ｓ１４４）。入力した人証情報等が認証ＩＣカード内に格納されている情報と一致するときに（Ｓ１４５）始めて人証情報の書き換えを許可する。

各人の認証に合格したときには、記録されていた人証情報を外部の記憶装置に転写し（Ｓ１４６）、書き換えの事実についてのログを認証ＩＣカード内に記録する（Ｓ１４７）。さらに、不要になった人証情報を消去し（Ｓ１４８）、所有者本人に人証情報を入力させ（Ｓ１４９）、新しい人証情報を認証ＩＣカードに格納する（Ｓ１５０）。

その後認証ＩＣカードの機能をテストして（Ｓ１５１）合格したら所有者に交付する（Ｓ１５２）。認証ＩＣカードが不良である場合は再度人証情報の書き換えを行ってテストに合格した場合に支給する。

なお、各人の認証に合格しない場合は不正なアクセスである可能性があるので人証情報の書き換えを拒絶する（Ｓ１５３）。

人証情報の読み出しや書き換えがあったときには、不正使用などの異常が起こったときにその原因になっている場合があるので、ログを取って認証ＩＣカード自体に格納しておくことが好ましい。

このように、本実施例の認証ＩＣカードは、人証情報の読み出しや書き換えに立会人などの承認を要求するようにすることができるので、窃盗や拾得により取得した認証ＩＣカードを盗用したり改竄することができないばかりか、認証ＩＣカードの発行装置、読み取り装置、書き換え装置などを自由に扱える者であっても立会人等の承認がない限り使用することができないので、認証ＩＣカードの安全性は極めて高い。

本発明のユーザ認証システムおよび認証ＩＣカードは錠前管理システムに適用することができる。

本発明の錠前管理システムの第１の実施例は、貸金庫管理に利用したもので、ＩＣカード内に登録された認証データを用いて本人認証を行うことにより、高い安全性を備えることができる。

第１５図を参照すると、鍵カード発行所３０１は貸金庫利用希望者に所定のＩＣカードを鍵カード３０２として発行し、貸金庫３０３は鍵カード３０２と利用者自身の認証データを読み取って認証に合格したときに鍵カード３０２が指定する金庫を解錠する。

鍵カード発行所３０１は、ホストコンピュータ３１１、ディスプレイやキーボードからなるデータ入出力装置３１２、人証データ入力装置３１３、鍵ＩＣカード発行用リーダライタ３１４を備えている。

金庫を借りたい者が利用を申し込むと、鍵カード発行所３０１の人証データ入力装置３１３から利用者の認証に使用する人証データを入力させる。

ホストコンピュータ３１１には、ソフトウエアとして鍵カード発行ソフトウエア、鍵管理ソフトウエア、認証データ登録ソフトウエアを搭載してある。鍵管理ソフトウエアは金庫の使用状況を把握し鍵カードに対応させる金庫を決めたり、錠前のセキュリティレベルを管理し認証情報の種類を指定するなどのほか、鍵カードの発行返却状況を管理し返却された鍵カードの記録内容を確実に抹消する。

データ入出力装置３１２はコンピュータシステムで通常必要とされるディスプレイ、キーボード、プリンタなどから構成される。

人証データ入力装置３１３は、指を押し付けると指紋パターンを抽出して分類する指紋読み取り器、マイクロフォンと声紋解析装置からなる声紋取得器、サインや符号を書き込むタブレット、など利用者個人が識別できる情報を入力する装置である。簡単な場合は、文字列暗号を入力するキーボードであっても良い。

鍵カード発行用リーダライタ３１４は、ＩＣカードリーダライタとＩＣカードリーダライタコマンドから構成される。

鍵カード発行所３０１は、貸す金庫を指定し、その金庫の利用を認める認証ＩＤと人証データ入力装置３１３で取得した利用者個人の本人認証データをＩＣカ

ード内のＣＰＵで管理されるメモリ領域に格納して、鍵カード３０２として発行し、利用者に貸与する。

鍵カード３０２はＣＰＵと内蔵メモリを備えたＩＣカードである。

貸金庫３０３には、ＩＣカードリーダライタと人証データ入力器を備えた解錠処理装置３３１と複数のロッカー式金庫３３２が設けられている。解錠処理装置３３１は金庫制御インタフェースを備え認証データ照合ソフトウエアを搭載している。金庫３３２は電気コントローラ付きで遠隔操作により施錠解錠ができる。

なお、異常を検知するセンサと異常時に警報を発生する通報装置を設備しておくと無人化しても安全を確保することができる。

貸金庫利用者は、貸金庫３０３のうちの指定された金庫３３２に物を収納して施錠する。一旦施錠した後は、利用者本人がその場で入力する人証データと利用者が提示する鍵カード３０２から読み取った認証データとが照合論理上認められた範囲内で一致している場合に限り、解錠処理装置３３１を介してその金庫を解錠する。

本管理システムによれば、鍵カード３０２が真正なものであってもそれを携帯している者が真正な利用者でなければ解錠することができないので、金庫の安全性が高く、管理人の立ち会いなどによる保証を併用するまでもない。したがって、貸金庫装置を無人管理あるいはそれに近い管理により運営することも可能となる。

なお、複数種類の認証情報を用いることにより、貸金庫のセキュリティレベルを選択して設定することも可能である。セキュリティレベルを選択できるようにしたものでは、金庫の利用者が金庫に収納する物の重要度と使い勝手を勘案して使用する認証情報を選択する。利用者が高いセキュリティを要求するときは署名により本人であることを確認することにしてもよいし、簡便さを重視した要求には文字列を使用すると決めても良い。

さらに、照合すべき情報を２種以上の組み合わせにすることにより極めて安全性の高い金庫とすることも可能である。

また、鍵カード３０２の発行時に利用する金庫を決めて、これに対応するＩＤをＩＣカード内に記入するようにすれば、未発行のＩＣカードが盗難にあっても盗用される危険は少ない。

BNSDOCID: <WO_____9960485A1_I_>

同じ錠前管理システムは、集中型セイフティボックスやロッカー、あるいは建物管理におけるキーボックスなど複数の者がアクセスする収納装置に利用することができる。

本発明の錠前管理システムの第２実施例は、保管庫の管理に利用したもので、ＩＣカードと手書きサインによる照合で本人確認を行い、保管庫内の重要物、薬品・劇物・毒薬などを安全に保管し、許可された者が許可された物だけを取り出せるようにするシステムである。

また、権限の無い者がアクセスしたときはセンサが検知して通報し、また外部からの攻撃にはシステムを安全サイドにロックするように回路構成を行うなど、保管庫の安全性と信頼性を十分に高める機能が付けられる。

第１６図は、保管庫に適用した錠前管理システムのブロック図である。

保管庫３０５は複数の保管室３５１，３５２，３５３に分かれており、保管室３５１内にさらに複数の小部屋あるいは保管棚３５４，３５５，３５６がある。

複数ある保管室それぞれと小部屋それぞれはセキュリティレベルが異なり、保管する物品の機密度に応じて保管室や小部屋を選別して使用することができる。

具体的な例を挙げると、たとえばある会社で保管庫３０５を所有していて、第１保管室３５１は社内でも一部の者にしか扱えない機密性の高い書類を保管する部屋とし特定の者にしか出入りを認めない。さらに、最高機密を要求される書類は第１保管室３５１中の第１の小部屋３５４に格納し、第１保管室３５１に出入りが認められる者の中でも、さらに第１小部屋３５４に入ることが認可される者しかアクセスさせない。また例えば第２小部屋３５５は人事関係資料を格納する部屋で、人事担当の責任者しかアクセスが認められず、第３小部屋３５６は経理書類の保管をする部屋で経理部の担当者しか出入りすることができないようにする。

また、第２保管室３５２は開発関係の資料を保管する部屋で、保管されている情報が外部に漏洩しないようにする必要があり、担当部局の者しか出入りさせない。一方、第３保管室３５３は、重要度の低い文書を収納しておく部屋で、社員であれば誰でも出入りできるが、出入りの記録が残るようにする。

また、セーフティボックス３５７のように独立した保管庫も同じシステムで管

理することができる。

本実施例の保管庫管理システムでも第１の実施例におけると同様に、各保管室、各小部屋ごとに資格を決め、これに合致する社員に対してＩＣカードで作成する鍵カード３０２を給付する。鍵カード３０２に基づく本人認証により資格を認められた社員だけが認められた部屋の解錠を行うことができるようにする。

すなわち、鍵カード３０２にはアクセスを認める錠前を指定する情報と人証データ入力装置で取得し所定の情報処理をした本人認証データがＩＣカード内のＣＰＵで管理されるメモリ領域に格納されている。

また、保管庫３０５には、鍵カード３０２を読み取るＩＣカードリーダライタ３４２と人証データ入力装置としてのタブレット３４３と情報を交換できる制御ユニット３４１、および各保管区分の錠前を制御するインターフェース３４４を備える錠前管理装置３０４が設けられている。

保管室３５１，３５２，３５３や小部屋３５４，３５５，３５６、またセーフティボックス３５７の扉には遠隔で操作できる電気錠が設備されていて、錠前管理装置３０４により施錠解錠の制御が行われる。なお、各扉には異常検知センサ３５８が設備されていて、部屋にアクセスがあると検知して信号を錠前管理装置３０４に送信する。

また、表示灯を設備しておきアクセスを認めた扉のところで点灯して、アクセス者に知らせるようにしても良い。

保管庫３０５を利用しようとするときは、利用者は鍵カード３０２をカードリーダライタ３４２に挿入してタブレット３４３に自分が登録時に決めた符号を入力する。制御ユニット３４１は、鍵カード３０２が真正なＩＣカードであることを確認し、どの錠前に対応するものかを、鍵カード３０２のＣＰＵを介して提供される記録内容から確認する。

次にタブレット３４３から入力されたサインなどの人証情報を鍵カード３０２から提供される本人認証データと照合して同一であるかどうかを判定する。認証データ照合ソフトウエアにより両者が合致することが確認されたときに、鍵カード３０２が指定する錠前についてアクセス権を有する人物と判定して、指定した錠前を解錠する。

BNSDOCID: <WO_____9960485A1_I_>

使用者が許可された管理領域以外にアクセスするとセンサが作動して警報を発生する。不正アクセスがあったときは、錠前が自動的に施錠されて不正アクセス者を室内に閉じ込めるようにしても良い。

なお、鍵カード３０２に基づいて解錠が許可されたときに、錠前または部屋や棚に設けられた表示灯の点灯により許可された対象を表示して、善意の者が誤ったアクセスをすることを防止するようにしても良い。

対象とする部屋のセキュリティの高さにより要求する認証の深さを予め決めておくことができる。単に鍵カード３０２を提示すればアクセスを認める水準であってもよく、予め入力した符号と形状、筆順、筆圧が一致することを要求しても良い。また、暗証番号とサインなど複合した保証を要求するより高度な水準であってもよい。

なお、これらの異なる水準のセキュリティに対応して複数の認証情報を１枚の鍵カード２に格納しておいて、アクセスする錠前毎に対応する認証データを読み出して照合するようにしても良い。

さらに、保管庫３０５の側に複数の異なる人証データ入力手段を備えておいて、必要とする認証の水準により使い分けることもできる。一般に高いセキュリティレベルに対応する認証情報は人証データ入力に手間が掛かるため、低度の安全性しか要求しない錠前ではより簡単な認証方法を用いて使用者の便宜を優先することもできる。

また、複数の種類から的確な認証情報を選択させることにより不正アクセスを排除しやすくすることもできる。どの種類の人証データをどの様に組み合わせるかを使用者自身に選択させるようにすると、他人の成り澄ましがさらに困難になり安全性がより向上する。

また、本管理システムでは錠前にアクセスする個人が明確に把握できるので、いつ、誰が、どの保管室（あるいは保管棚等）にアクセスしたかを自動的に記録しておくことができる。

なお、停電した時や電源ケーブルが切断されたときには、システムは機密上安全側にロックされるようになっている。保管庫を破壊行為などを含め異常が起こったときには管理室に警報する機構を備えることが好ましい。

なお、緊急時にはロックを解除できる管理者用の認証レベルを備えておくことが好ましい。

本実施例の説明は、書類の管理について記載したが、薬品を危険度に従って管理する薬品庫、薬品棚やロッカーなどの要求に対しても全く同じ実施例を適用することができる。

産業上の利用可能性

以上のように、本発明に係るユーザ認証システムを用いれば、認証利用所において直接にユーザが入力する人証情報と認証票内の生物学的特徴データを照合し、より高度の保証を欲するときに上位の認証局に人証情報の一部を伝送してユーザ認証をするため、情報処理の大部分を認証利用所で行って通信回路に大きな負荷をかけることなく、安全性の要求水準に対応したユーザ認証を得ることができる。また、人証情報を分割することにより侵襲に対して極めて強いユーザ認証システムの構築が可能となる。

また、本発明の認証ＩＣカードは、ＣＰＵを介して情報のアクセスを行うため、ファイルのアクセス権限を任意に設定して、人証情報を活用して不正なアクセスを排除するので、所持者のプライバシーが確実に保護でき、またサービスの提供者等にとっても安全性の高い取引が可能となる。また、多数のサービス等を利用する場合でも携帯するカードの数を少なくすることができる。

さらに、本発明の認証ＩＣカードは、発行時などに第２の人物の承認を要求するようにできるので、盗用等の危険が極めて小さく、安全性が高い。

また、本発明の錠前管理システムは、認可された人物の認証を正しく行うため保管物の高度の安全が確保でき、従来より安全度の高い保管庫管理システムや貸金庫管理システムを構築することができる。

BNSDOCID: <WO_____9960485A1_I_>

請求の範囲

1．ユーザの個体を区別する生物学的特徴データを取得する情報取込み装置を備えた登録所と、該ユーザに対してその生物学的特徴データのうち分割された一部を記録したユーザ認証票を発行する認証票発行所と、該ユーザ認証票の情報を読み取る認証票読取り装置とユーザの生物学的特徴データを入力する人証取得装置を設けた認証利用所と該認証利用所と情報通信路で接続された少なくとも１個の認証局を備えてなるユーザ認証システムであって、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を該認証局に記録しておいて、該認証利用所において前記認証票読取り装置で読みとるユーザ認証票の記録内容と前記人証取得装置に入力された前記ユーザの生物学的特徴データを比較することにより該ユーザが核ユーザ認証票の正当な所有者であることを認証すると共に、さらに高度な認証を行うときには前記認証局が前記認証利用所からの照会に応えて前記ユーザ認証票において欠けている生物学的特徴データの部分を比較して認証した結果を前記認証利用所に送付することを特徴とするユーザ認証システム。

2．前記認証利用所における認証のための演算を前記ユーザ認証票の演算機能を用いて行うことを特徴とする請求の範囲第１項記載のユーザ認証システム。

3．前記情報通信路に流す情報は暗号化することを特徴とする請求の範囲第１項または第２項記載のユーザ認証システム。

4．前記２個以上の認証局が、前記登録所において取得したユーザの生物学的特徴データのうち前記ユーザ認証票に記録しない部分を分割して記録しておいて、各認証局毎に前記認証利用所もしくは他の認証局からの照会に応えて自己の記憶する生物学的特徴データの部分を比較して認証するようにしたことを特徴とする請求の範囲第１項ないし第３項のいずれかに記載のユーザ認証システム。

5．前記ユーザ認証システムが前記登録所において取得したユーザの生物学的特徴データを記録する記憶装置を設けた認証局を備えることを特徴とする請求の範囲第１項ないし第４項のいずれかに記載のユーザ認証システム。

6．前記生物学的特徴データとして複数のものを登録して、入力されたデータにより異なる取引を行うことを特徴とする請求の範囲第１項から第５項のいずれか

に記載のユーザ認証システム。

7．ユーザ認証票に記録された情報を読み取る認証票読取り装置と、ユーザの生物学的特徴データを入力する人証取得装置と、前記認証票読取り装置で読み取ったユーザ認証票に記録されている生物学的特徴データと前記人証取得装置に入力された前記ユーザの生物学的特徴データを比較して合否を判定する判定装置と、人証取得装置に入力されたユーザの生物学的特徴データの少なくとも一部を外部の認証局に送信し認証の判定結果を受け取る通信装置と、判定結果を出力する表示装置を備えるユーザ認証装置。

8．ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ＩＣカードであって、外部から前記アプリケーションファイルに記録された情報の提示要求があったときに、前記ＣＰＵが外部から入力される人証情報と前記認証ファイルに格納された人証情報と対比して認証の深さを確認し、合格したときに前記ＣＰＵを介して前記アプリケーションファイルへのアクセスが認められることを特徴とする認証ＩＣカード。

9．ＣＰＵと人証情報を格納した認証ファイルと認証の深さに応じて分類されたアプリケーションファイルを備えた認証ＩＣカードであって、外部から前記アプリケーションファイルに記録された情報の提示要求があったときに、前記ＣＰＵが前記認証ファイルに格納された人証情報を出力して、外部装置から受け取る判定結果に基づいて、前記ＣＰＵを介して前記アプリケーションファイルへのアクセスを行うことを特徴とする認証ＩＣカード。

１０．前記アプリケーションファイルには対象とする取引の権限を示す固有のＩＤが記録してあることを特徴とする請求の範囲第８項または第９項記載の認証ＩＣカード。

１１．前記アプリケーションファイルへのアクセスは、ファイル毎に予めアクセス資格を登録し、認定された資格者に対してのみ認めるようにしたことを特徴とする請求の範囲第８項から第１０項のいずれかに記載の認証ＩＣカード。

１２．ＣＰＵと、人証情報もしくは人証情報と認証情報を格納した認証ファイルと、認証の深さに応じて分類されたジョブプログラムやデータを格納したアプリケーションファイルとを備え、外部から前記アプリケーションファイルへのアク

セスの要求があったときに、前記認証ファイルに格納された人証情報に基づいて真偽を判定した結果により該アクセスを認める認証ＩＣカードであって、前記認証ファイルにカードで認証する第１の人物以外に少なくとも１人の第２の人物の人証情報または少なくとも１つの主体の認証情報を格納し、該第２人物または主体の認証を要求するジョブあるいはデータを予め決めてあって、該第２人物または主体の認証を要求するジョブあるいはデータについて実行あるいは提示の要求があったときに、前記第２人物または主体によって外部から入力される人証情報または認証情報と前記認証ファイルに格納された人証情報または認証情報とを対比して認証に合格したときに前記ＣＰＵを介して前記ジョブの実行やデータの提示を認めるようにしたことを特徴とする認証ＩＣカード。

１３．前記ＣＰＵが前記認証ファイルに格納された人証情報または認証情報を外部装置に出力して、該外部装置から受け取る判定結果に基づいて、前記ＣＰＵを介して前記アプリケーションファイルへのアクセスを行うことを特徴とする請求の範囲第１２項記載の認証ＩＣカード。

１４．前記人物または主体の認証を前記第１人物および前記第２人物または前記主体の両者について実行して両者共に合格したときに始めて前記アプリケーションファイルへのアクセスが認められるようにしたことを特徴とする請求の範囲第１２項または第１３項に記載の認証ＩＣカード。

１５．さらに前記認証ＩＣカードが認証の内容を記録した電子証明用ファイルを有し、前記アプリケーションファイルへのアクセスを行うときに利用された認証の内容を表す電子証明書を提示することができるようにしたことを特徴とする請求の範囲第１２項から第１４項のいずれかに記載の認証ＩＣカード。

１６．ＩＣカードリーダと人証データ入力装置を備え、利用者の本人認証データを記録したＩＣカードを前記ＩＣカードリーダで読み、前記人証データ入力装置から入力された人証データと前記ＩＣカードに記録された本人認証データを照合して認証に合格したときに対応する錠前を解錠することを特徴とする錠前管理システム。

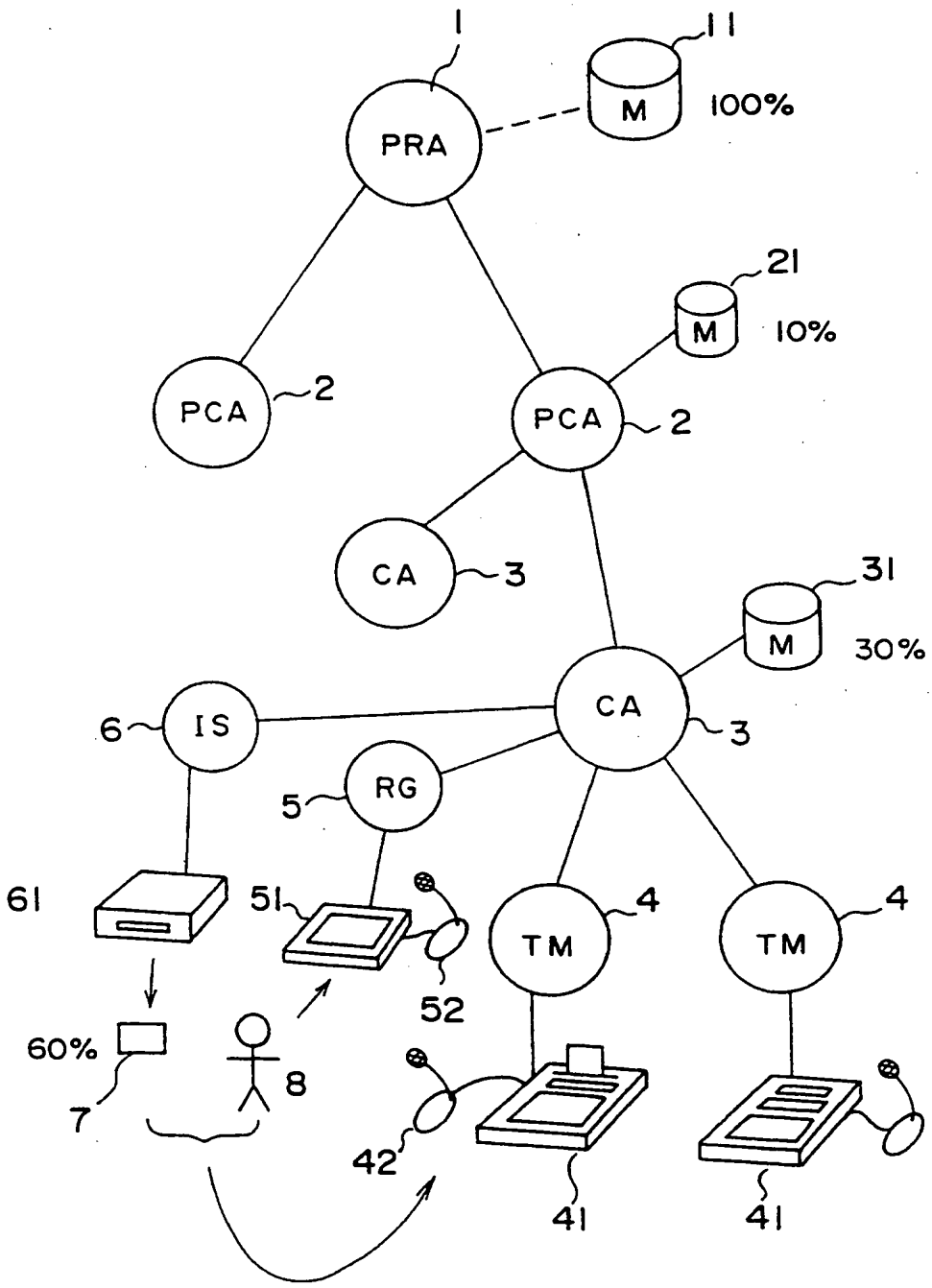
１７．前記ＩＣカードに記録される本人認証データが、利用者が所有する生体情報データもしくは利用者が作成する情報データであることを特徴とする請求の範

囲第１６項記載の錠前管理システム。

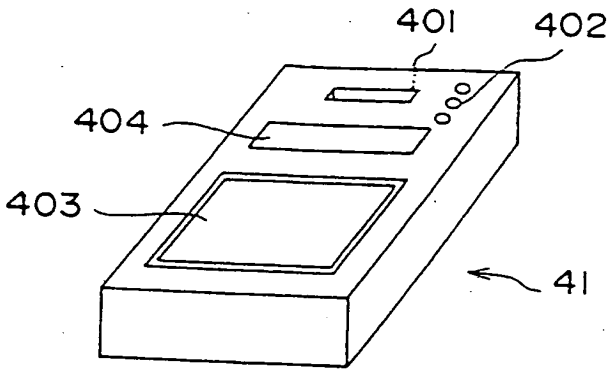
１８．前記ＩＣカードに記録できる本人認証データの種類が複数あって、選択して記録できることを特徴とする請求の範囲第１６項または第１７項記載の錠前管理システム。

１９．前記錠前が複数の管理区分に分けられた保管庫の管理区分毎に設けられていて管理区分毎に適用する本人認証データが選択できることを特徴とする請求の範囲第１８項記載の錠前管理システム。

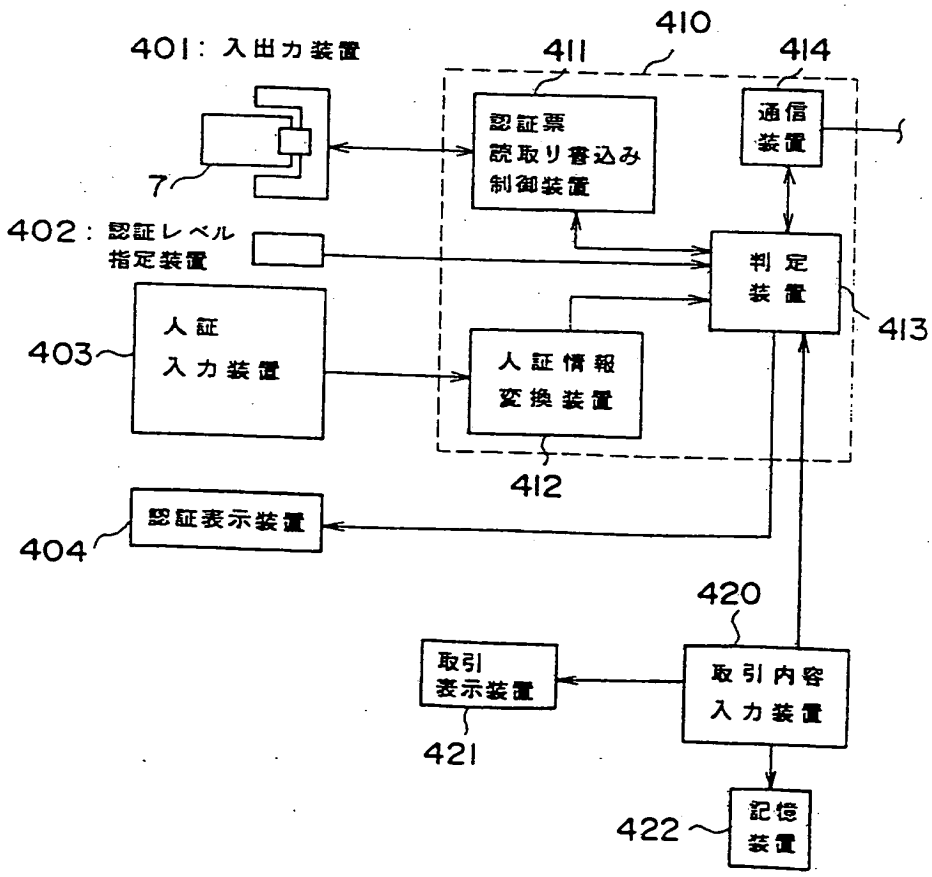
第 1 図


1
11
M
100%
PRA
21
M
10%
PCA
2
PCA
2
CA
3
31
M
30%
CA
3
6
IS
5
RG
61
51
52
TM
4
TM
4
60%
7
8
42
41
41

第 2 図

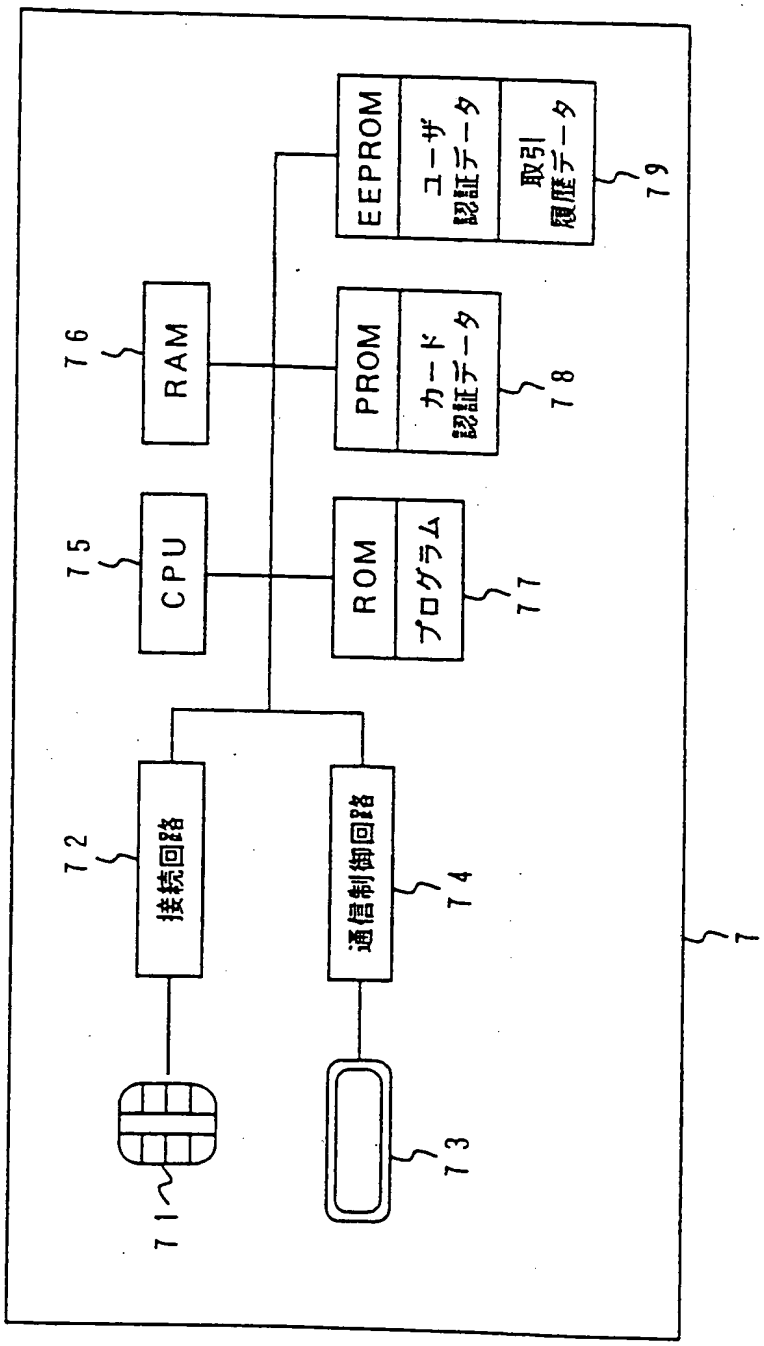


第 3 図



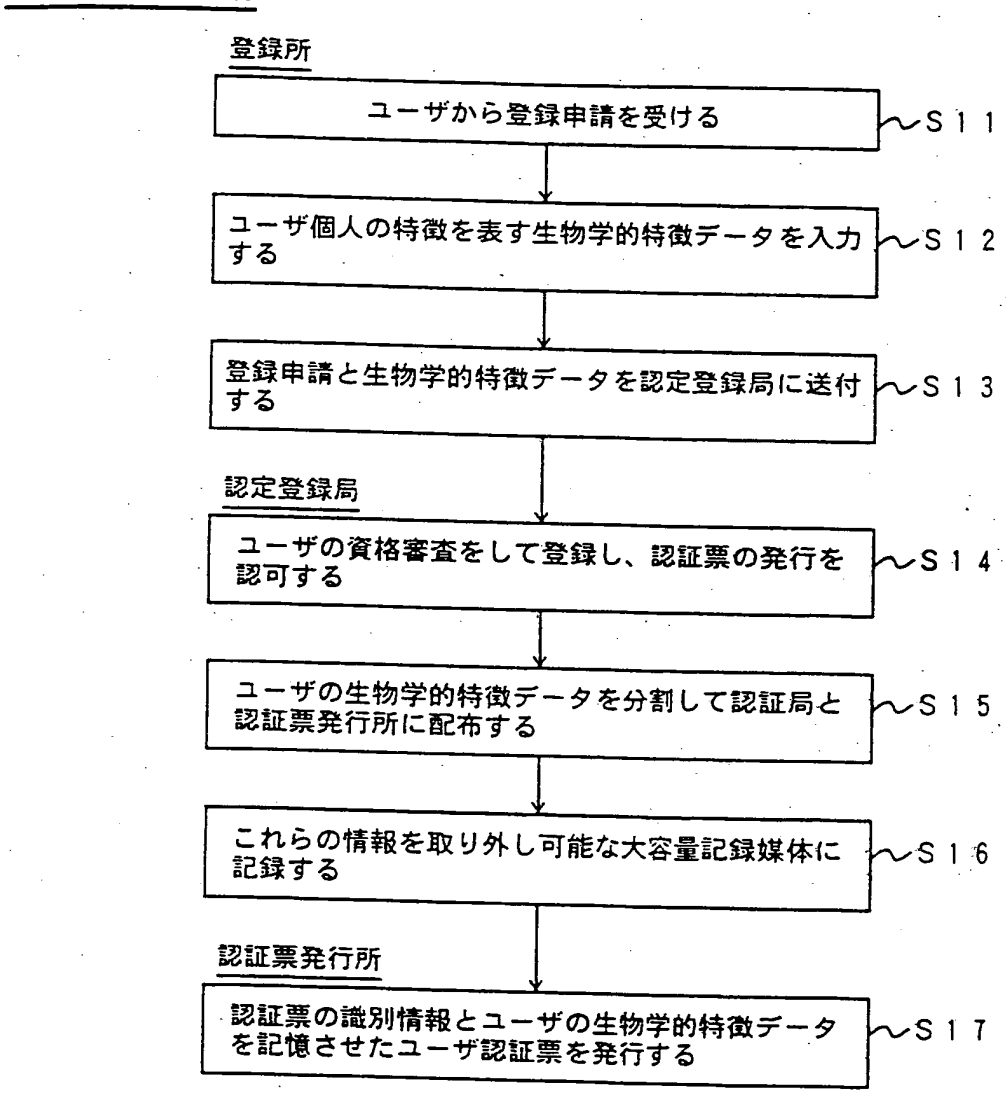
BNSDOCID: <WO_____9960485A1_I_>

第 4 図

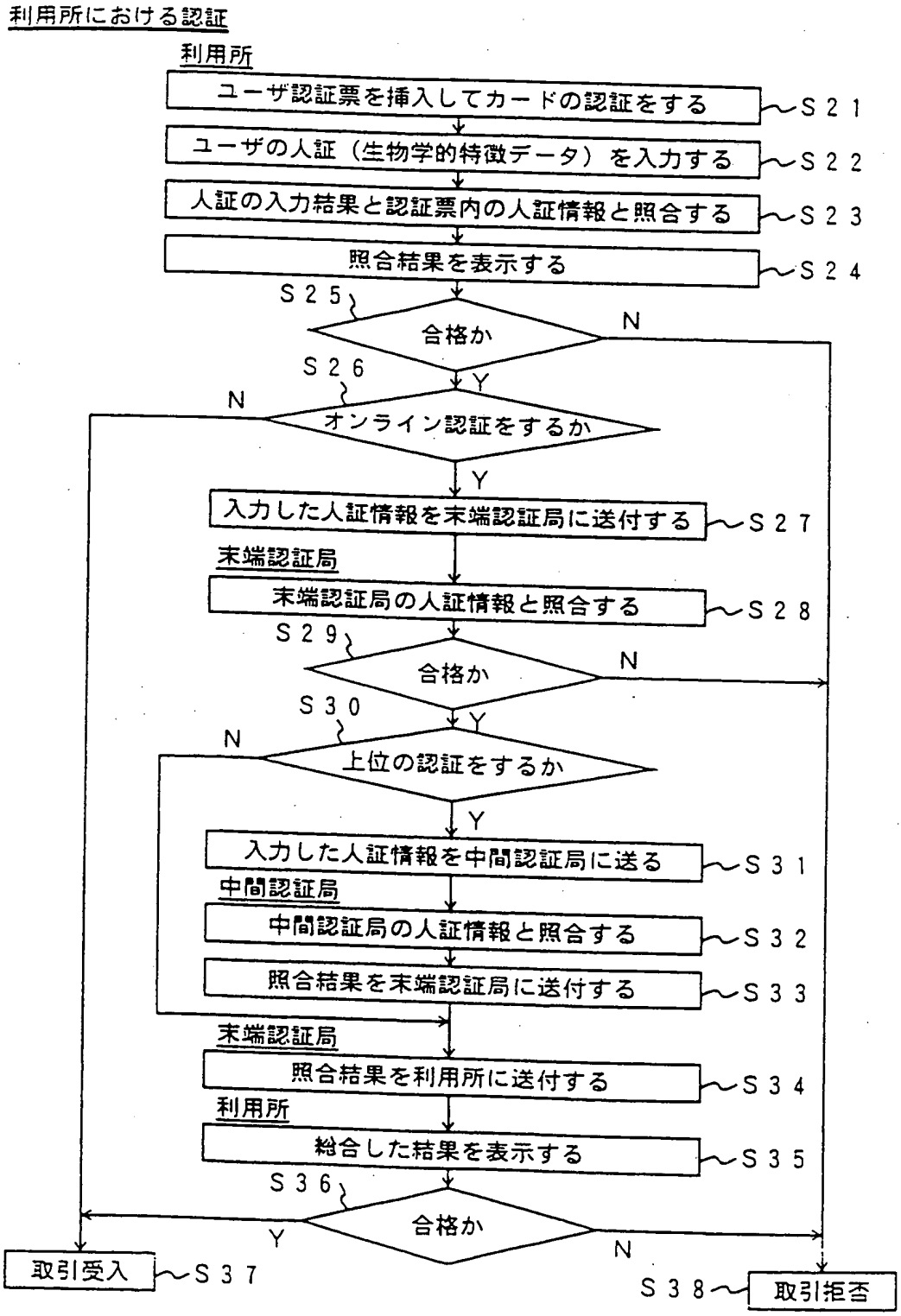


BNSDOCID: <WO_____9960485A1_I_>

第５図

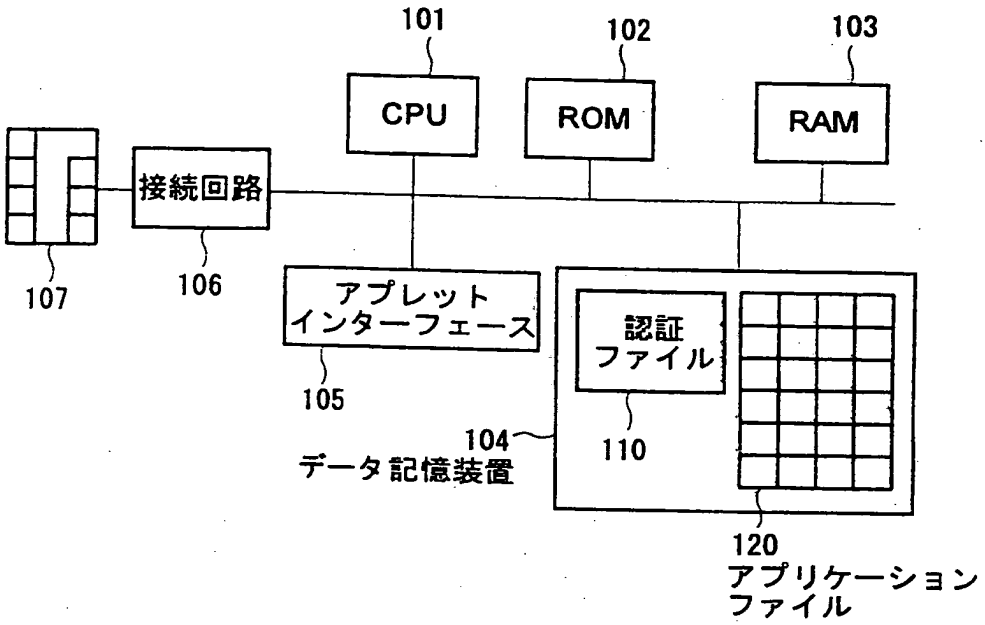

ユーザ認証票の発行
登録所
ユーザから登録申請を受ける
S11
ユーザ個人の特徴を表す生物学的特徴データを入力する
S12
登録申請と生物学的特徴データを認定登録局に送付する
S13
認定登録局
ユーザの資格審査をして登録し、認証票の発行を認可する
S14
ユーザの生物学的特徴データを分割して認証局と認証票発行所に配布する
S15
これらの情報を取り外し可能な大容量記録媒体に記録する
S16
認証票発行所
認証票の識別情報とユーザの生物学的特徴データを記憶させたユーザ認証票を発行する
S17

第 6 図

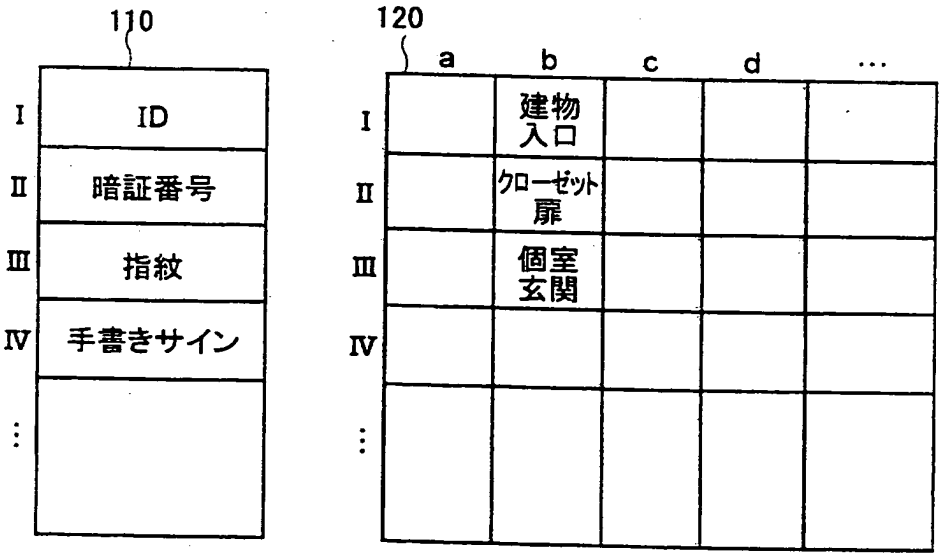


BNSDOCID: <WO_____9960485A1_I_>

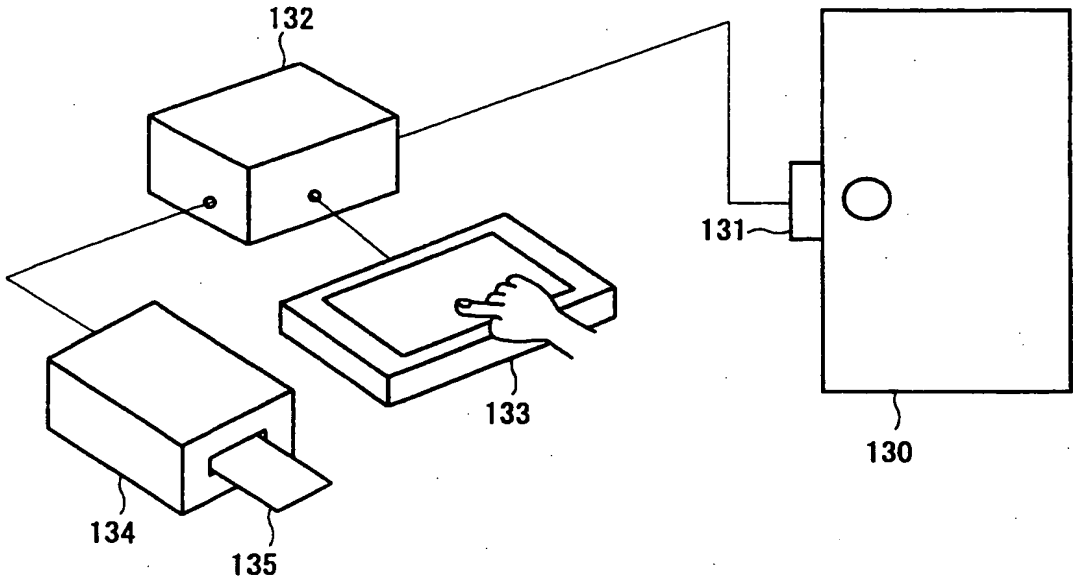
第 7 図


101
CPU
102
ROM
103
RAM
接続回路
107
106
アプレット
インターフェース
105
認証
ファイル
110
104
データ記憶装置
120
アプリケーション
ファイル

第 8 図

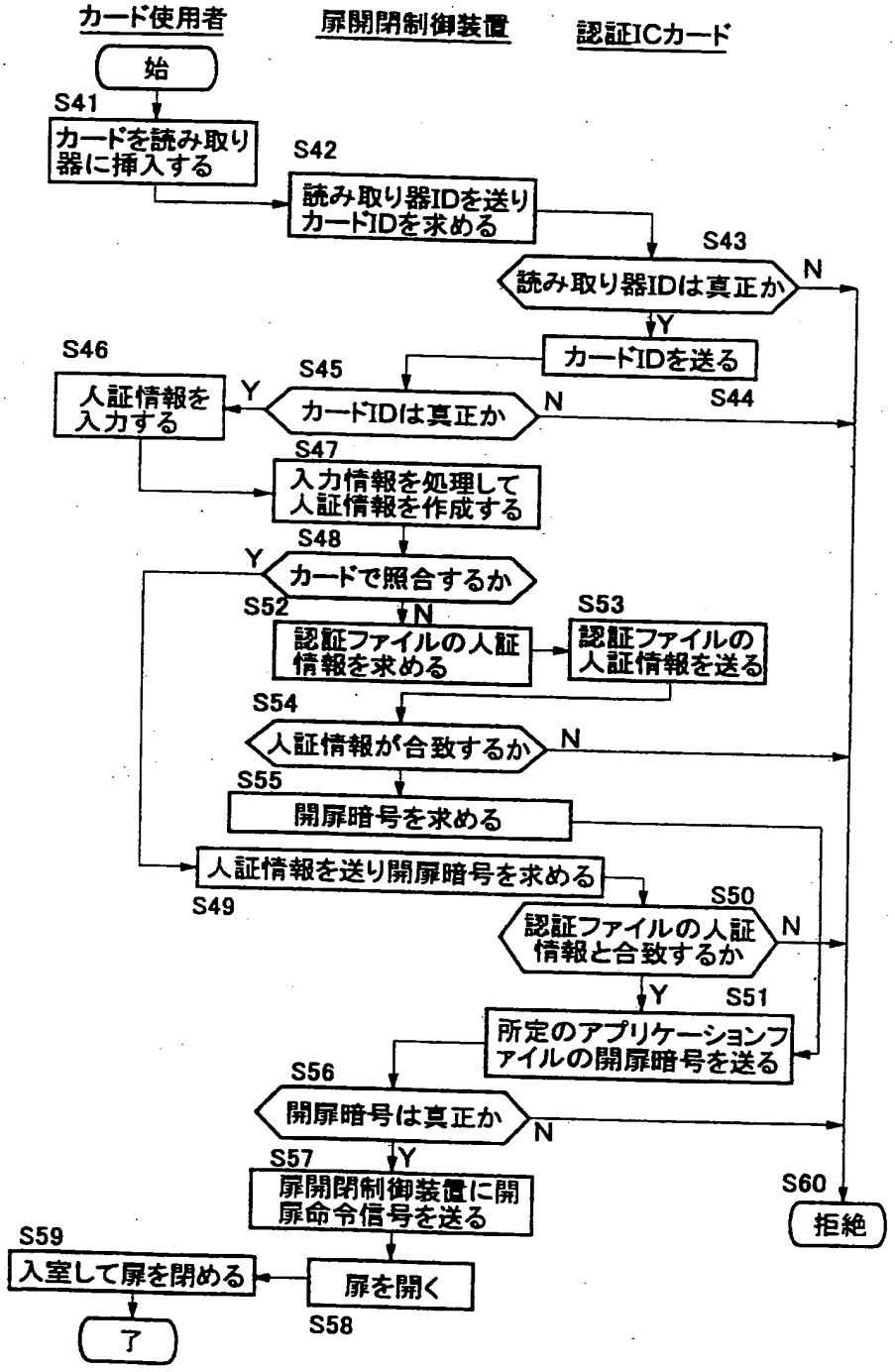

110
I
ID
II
暗証番号
III
指紋
IV
手書きサイン
120
a
b
c
d
…
I
建物
入口
II
クローゼット
扉
III
個室
玄関
IV

第 9 図

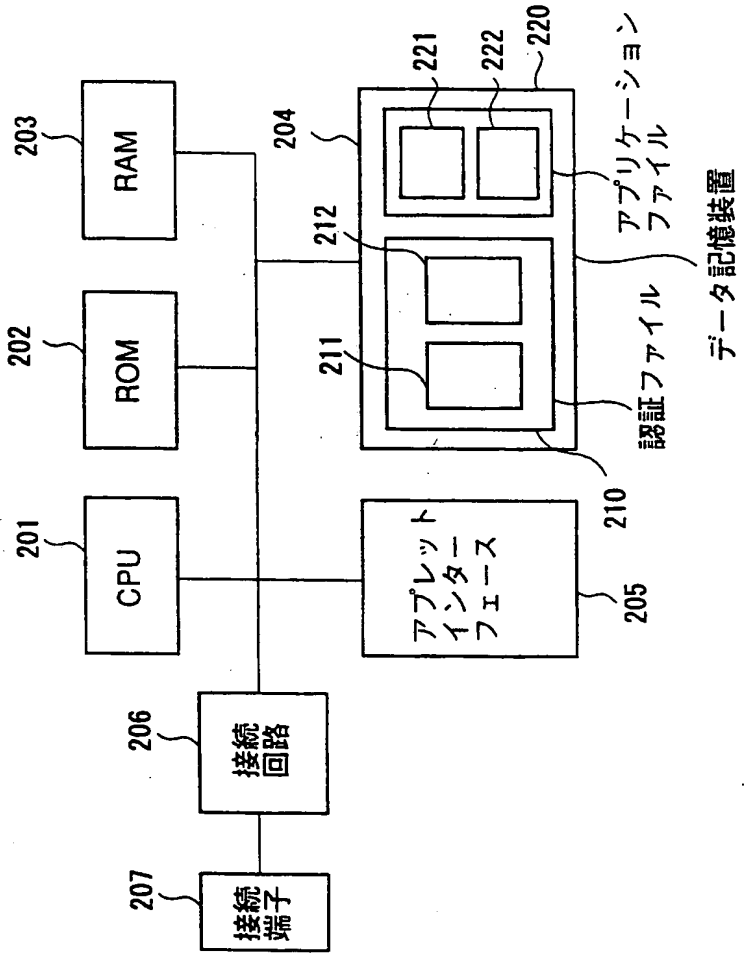


BNSDOCID: <WO_____9960485A1_I_>

第１０図


カード使用者
扉開閉制御装置
認証ICカード
始
S41
カードを読み取り器に挿入する
S42
読み取り器IDを送りカードIDを求める
S43
読み取り器IDは真正か
N
Y
カードIDを送る
S46
人証情報を入力する
Y
S45
カードIDは真正か
N
S44
S47
入力情報を処理して人証情報を作成する
S48
Y
カードで照合するか
S52
N
認証ファイルの人証情報を求める
S53
認証ファイルの人証情報を送る
S54
人証情報が合致するか
N
S55
開扉暗号を求める
人証情報を送り開扉暗号を求める
S49
S50
認証ファイルの人証情報と合致するか
N
Y
S51
所定のアプリケーションファイルの開扉暗号を送る
S56
開扉暗号は真正か
N
Y
S57
扉開閉制御装置に開扉命令信号を送る
S60
拒絶
S59
入室して扉を閉める
扉を開く
S58
了

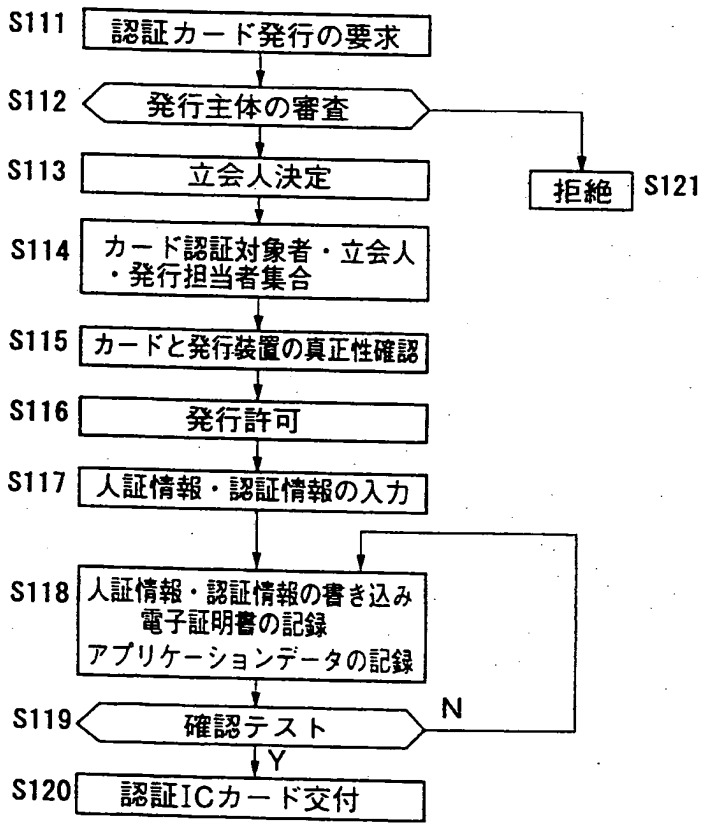
第11図



BNSDOCID: <WO_____9960485A1_I_>

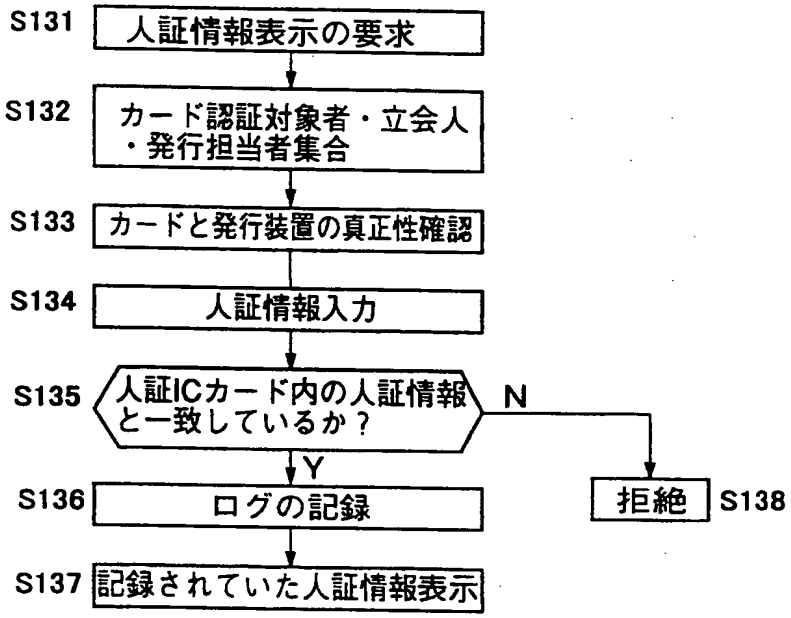
第12図

認証ICカード発行プロセス



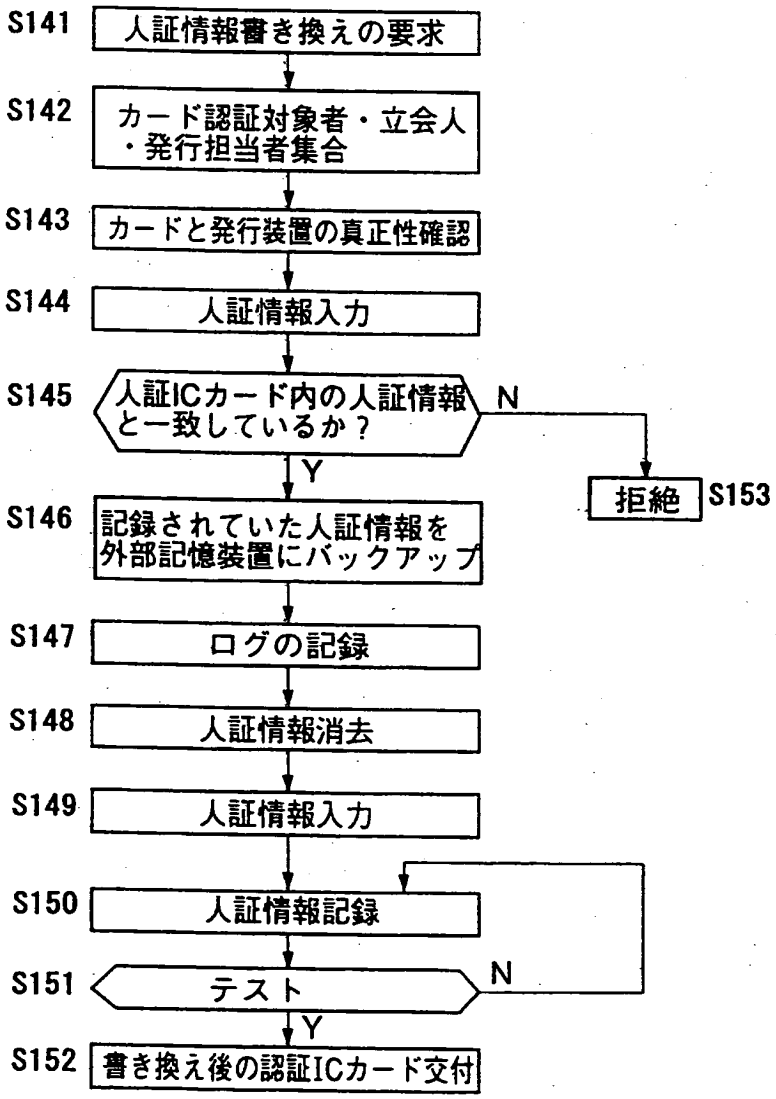
第13図

人証情報確認プロセス

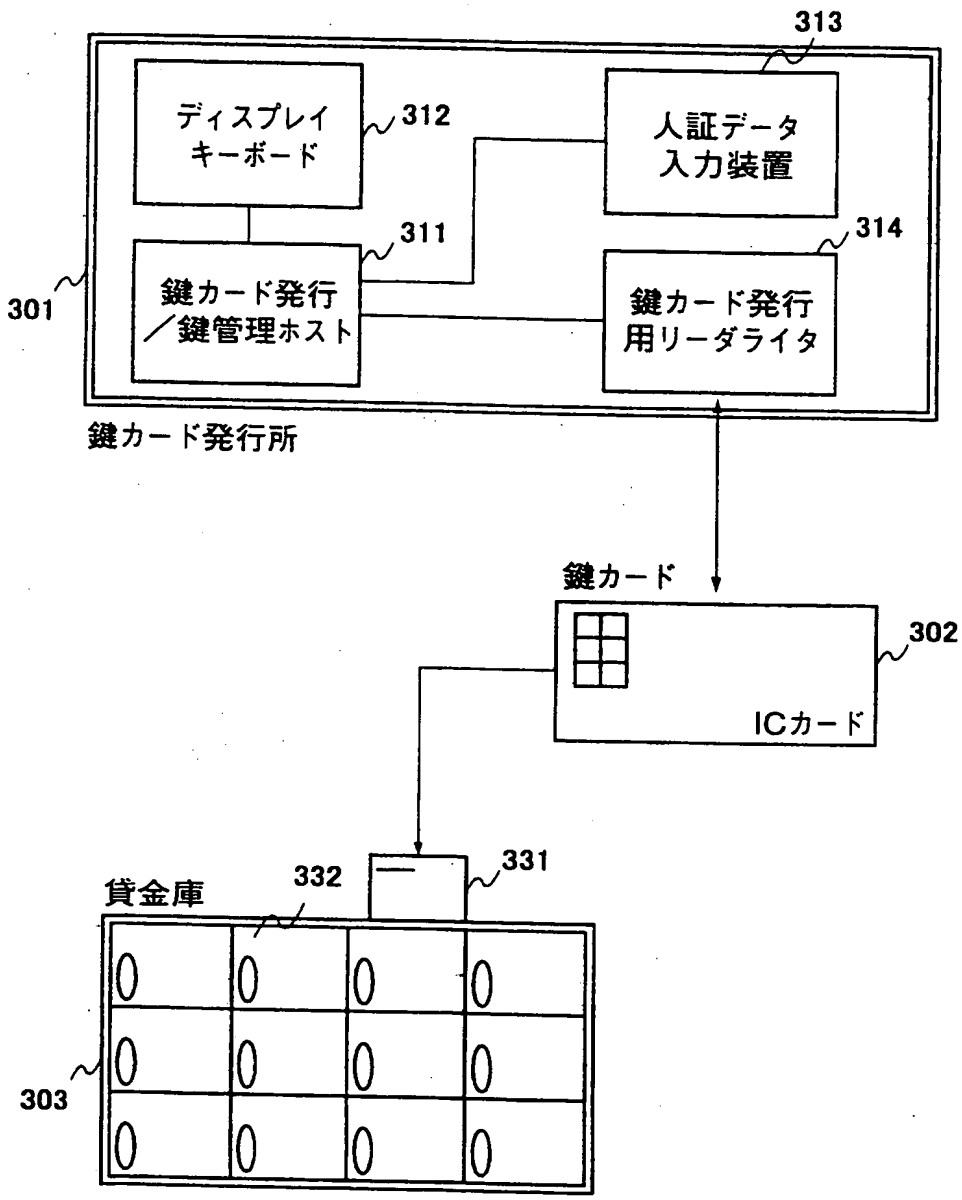


第14図

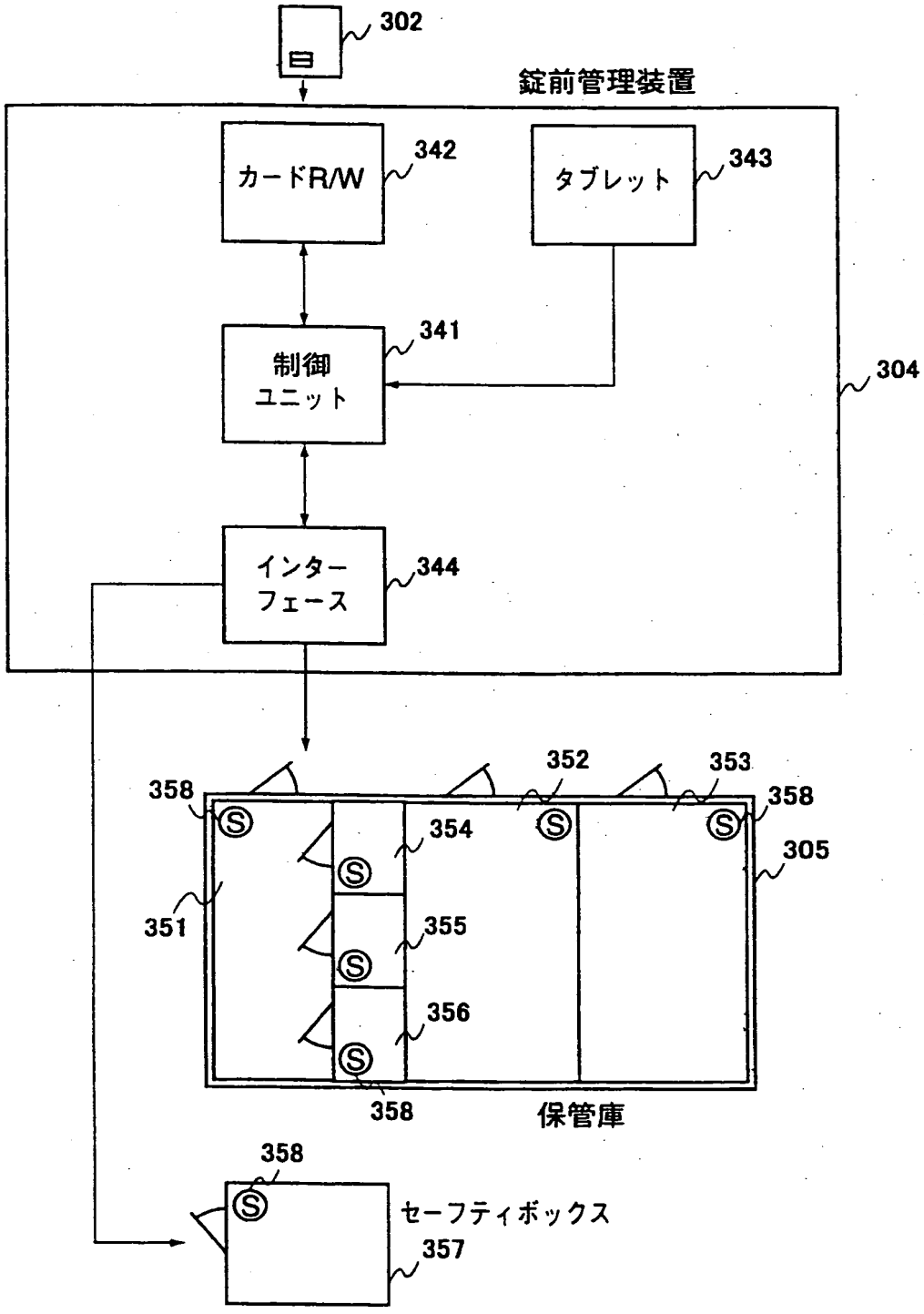
人証情報書き換えプロセス



第15図


313
ディスプレイ
キーボード
312
人証データ
入力装置
311
314
301
鍵カード発行
／鍵管理ホスト
鍵カード発行
用リーダライタ
鍵カード発行所
鍵カード
302
ICカード
貸金庫
332
331
303

第16図


302
錠前管理装置
カードR/W
342
タブレット
343
制御
ユニット
341
304
インター
フェース
344
352
353
358
358
354
305
351
355
356
358
保管庫
358
セーフティボックス
357

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02599

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G06F15/00, 330, G06K19/00, E05B49/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G06F15/00, 330, G06K19/00, E05B49/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
JICST File on Science and Technology (Ninshou, Bunsan, Bunkatsu)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 57-55468, A (Hitachi,Ltd.), 2 April, 1982 (02. 04. 82) (Family: none)	1-7
A	JP, 7-28755, A (Toshiba Corp.), 31 January, 1995 (31. 01. 95) (Family: none)	1-7
A	JP, 7-64911, A (Sharp Corp.), 10 March, 1995 (10. 03. 95) (Family: none)	1-7
Y	JP, 1-224888, A (NEC Corp.), 7 September, 1989 (07. 09. 89) (Family: none)	8-15
Y	JP, 8-30745, A (Nippon Telegraph & Telephone Corp.), 2 February, 1996 (02. 02. 96) (Family: none)	8-15
Y	JP, 62-295194, A (Toshiba Corp.), 22 December, 1987 (22. 12. 87) (Family: none)	12-15
X Y	JP, 63-32075, A (Mitsubishi Electric Corp.), 10 February, 1988 (10. 02. 88) (Family: none)	16-18 19

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 July, 1999 (21. 07. 99)	3 August, 1999 (03. 08. 99)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

BNSDOCID: <WO_____9960485A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/02599

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 61-183586, A (Mitsubishi Electric Corp.), 16 August, 1986 (16. 08. 86) (Family: none)	19

国際調査報告

国際出願番号　PCT／JP99／02599

A.　発明の属する分野の分類（国際特許分類（IPC））
Int. Cl⁶　G06F15／00，330
G06K19／00
E05B49／00

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））
Int. Cl⁶　G06F15／00，330
G06K19／00
E05B49／00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1926－1996年
日本国公開実用新案公報　1971－1999年
日本国実用新案登録公報　1996－1999年
日本国登録実用新案公報　1994－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）
JICST科学技術文献ファイル（認証、分散、分割）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP, 57-55468, A（株式会社日立製作所）2.4月.1982(02.04.82)（ファミリーなし）	1～7
A	JP, 7-28755, A（株式会社東芝）31.1月.1995(31.01.95)（ファミリーなし）	1～7
A	JP, 7-64911, A（シャープ株式会社）10.3月.1995(10.03.95)（ファミリーなし）	1～7

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
21．07．99	03.08.99

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5L	9740
日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	高瀬　勤		
	電話番号　03－3581－1101　内線　3560		

様式PCT／ISA／210（第2ページ）（1998年7月）

BNSDOCID: <WO_____9960485A1_I_>

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０２５９９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	JP, 1-224888, A（日本電気株式会社）7.9月.1989(07.09.89) (ファミリーなし)	８～１５
Ｙ	JP, 8-30745, A（日本電信電話株式会社）2.2月.1996(02.02.96) (ファミリーなし)	８～１５
Ｙ	JP, 62-295194, A（株式会社東芝）22.12月.1987(22.12.87) (ファミリーなし)	１２～１５
Ｘ Ｙ	JP, 63-32075, A（三菱電機株式会社）10.2月.1988(10.02.88) (ファミリーなし)	１６～１８ １９
Ｙ	JP, 61-183586, A（三菱電機株式会社）16.8月.1986(16.08.86) (ファミリーなし)	１９